From: Sheehan, Erin (DOT)
To: Clements Jr, Robert F (POL)
Subject: AAMVA 2020 License Plate Standard Final (4) (002).pdf
Date: Wednesday, May 26, 2021 2:09:15 PM
Attachments: AAMVA 2020 License Plate Standard_Final (4) (002).pdf

---

2.2 Character Sizing and Placement Characters are at least 2.5 inches in height, proportionally wide, and spaced no less than 0.25 inches apart. Character stroke weight (thickness of lines) is between 0.2 and 0.4 inches. Characters are positioned on the license plate no less than 1.25 inches away from the top and bottom edges of the license plate.

From:	Chris Perez
To:	McCarthy, Steven (POL)
Cc:	Mason, Christopher (POL); Warmington, Scott (POL); Quinn, Dermot (POL); Kevin Coughlin; Small, Michelle (POL); Venkatachalam, Krishna (EPS); Robles, Francis Jr. (POL); Connor, Debora (POL); Ryan Garofano
Subject:	ALPR & 4RE Decision
Date:	Wednesday, March 17, 2021 11:30:43 AM
Attachments:	L5Q Quick Deploy LPR System Data Sheet.pdf Mobile Companion Sheet.pdf L5F Fixed LPR Data Sheet.pdf Mobile LPR Data Sheet.pdf

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

Captain McCarthy,

Your email to the group was forwarded over to me from the WatchGuard staff so I just wanted to take a moment to respond. Thanks for meeting my colleague Ryan Garofano yesterday and evaluating the 4RE LPR solution. As you referenced, the field of view for the 4RE is too broad, and asking it to do both LPR + evidence collection has seemed to be a tough ask.

This was the first iteration of the integration we hope to achieve with our partnership with WatchGuard. We are building out a new version of this in the future and this feedback is extremely valuable.

One thing to clarify is that in your email you stated, "What it does underscore is that the Vigilant system needs a purpose-built camera for robust ALPR." I just wanted to note that we do in fact have a series of robust LPR cameras that we've been selling on the market, many of which have been deployed throughout the state of Massachusetts. With your LPR data subscription you'll be able to see both the commercial data *and* all of our cameras deployed by police departments around the country.

I attached some information on our fixed cameras, our solar/quick deploy option, mobile cameras, and mobile app, all of which are integrated into our system. If you're open to further discussions about expanding, want some flexibility, or would like to demo our robust equipment, we would certainly welcome them. I understand you guys have utilized PIPS in the past, but with our recent updates I'm confident you would see an enhancement in both hardware and software functionality. Keep in mind we can always integrate your existing data to avoid having to use 2 separate backends.

If you ever have any questions, please feel free to reach out to either me or Ryan and we'd be happy to discuss.

Happy St. Patty's Day.

Thanks,

Chris Perez
Eastern US Sales Director
Video Security & Analytics
Vigilant Solutions



m: (516) 859-1520
TEMPORARY NUMBER through 3/18 - (242) 824-8837

Grant Assistance | Training | LinkedIn

Support: (925) 398-2079 | Email Support

For more information on how and why we collect your personal information, please visit our Privacy Policy.

From: Justin Dutra
To: dmartin@tivertonpoliceri.com; jpepjonovich@quincyma.gov; cgraham@nespin.riss.net; Clement, Michael (POL); Paul Gauvin; walter_correia@warehampolice.com
Subject: ALPR Access
Date: Friday, October 29, 2021 11:15:53 AM
Attachments: FLOCK MOU.docx

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

Good Morning,

In response to recent requests for access to Cranston Police ALPR network, I have prepared a MOU which has been attached to this email. Please read, sign, and return for immediate access.

Thank you.

Respectfully,

Lieutenant Justin T. Dutra
Special Projects Lieutenant
Cranston Police Department
Desk (401) 477-5035
Cell (401) [redacted]
Email: jdutra@cranstonpoliceri.com

From: Egnitz, Brian (POL)
To: Wilcox, Christopher (POL)
Subject: ALPR Bills
Date: Thursday, June 24, 2021 9:14:46 AM
Attachments: Re ALPR Proposed Legislation.msg
Fwd ALPR Proposed Legislation.msg

From: John Tedona
To: Pack, Noah (POL)
Subject: ALPR Equipment PDFs
Date: Monday, November 29, 2021 1:44:42 PM
Attachments: image001.png
image002.png
image003.png
P720 Mobile ALPR.pdf
Iris Data sheet US.pdf

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

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Bender, Sean (POL)
To: Thibault, Amy (POL)
Cc: Smith, Eleanor (POL)
Subject: Analysis Toolkit
Date: Wednesday, January 27, 2021 3:46:13 PM
Attachments: Analyst Professional Development Road Map.pdf

Good Afternoon, Amy/Elly -

I don't know that anyone else would find this interesting, but the NFCA Conference block on *Managing Your Intelligence Analysis Services Toward a Successful Result* referred a couple times to the *Analyst Professional Development Roadmap.* I'm sure most have seen or read the document at this point, but it links to the Office of Justice Programs - Analysis Toolkit site https://it.ojp.gov/AT/ which has *a lot* of interesting tools and resources for categories like policy, technology, training, etc. There are some good reads on ALPR/FR policy, Use of Social Media in Intelligence/Investigative Activities, P/CRCL, etc.

> Analysis Toolkit - Office of Justice Programs
>
> Notice of Federal Funding and Federal Disclaimer. This website is funded through a grant from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse this website (including, without limitation, its content, technical infrastructure ...
>
> it.ojp.gov

Respectfully,

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

From: Peter Crary
To: Mitchell, Timothy (EPS); Egnitz, Brian (POL)
Subject: aws snowball
Date: Friday, September 17, 2021 12:29:02 PM
Attachments: image007.png
image008.png
image009.png
snowball-edge-data-migration-guide.pdf

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

Peter Crary
Global R&D Director, ANPR/ALPR

Mobile: + 865 386 3821
Email: pcrary@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

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

From: LPR
To: Brooks, Brian (POL); Hersey, Kevin
Cc: Castaneda, Robert E.(Eric); Hurst, Donald S (Stuart)
Subject: DEASIL LPR MOU Data Share - Follow-up
Date: Monday, September 13, 2021 1:16:37 PM
Attachments: image001.png
image002.png
image004.png
CC APPROVED LPR Standard Data-Sharing MOU Template 2020-07-09.doc
07.02.21 EPIC-DEASIL.pdf

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

Good afternoon Lieutenant Brooks,

I was provided your name by SA Hersey of the New England Office, and I thought to follow up on our request to integrate your local aLPR data (Vendor: UKN) with the National License Plate Reader Program (DEASIL) here at the El Paso Intelligence Center (EPIC). I've attached the pre-approved Chief Council Data Share MOU for your review – but understand if you might have any logistical questions.

As we approach the end of our fiscal year, we are reviewing prior inquires from various agencies and identified your agency as one to follow up on. We are abundantly aware that the past year has been a trying time for all, and understand that this request may have been earmarked for a later date. At your convenience, can you indicate whether you plan to move forward with data share, or whether you'd like to be taken off of our list of interest?

Do know that this is not a one way flow of data, you and your colleagues are able to utilize DEASIL (which is upto about 3,000 site locations across the antion) on your own or through our 24hr Watch Unit, free of charge, once you've been vetted through EPIC. Again, I am available for any questions or concerns you may have. We look forward to hearing from you!

Thank you,

Cari N. Schieno | Program Analyst
DEASIL | National License Plate Reader Program (LPR)
El Paso Intelligence Center (EPIC)
Desk: (571) 387-4220 | Cell: (915) [redacted]
Cari.N.Schieno@dea.gov
"Do right and fear not"

"We'd love to hear any success stories from you, the users. These justify the coverage and growth of this program!"
You can send your stories to LPR@usdoj.gov or to cari.n.schieno@usdoj.gov
DEASIL Password/Account reset LPR@usdoj.gov

If you or a partner agency utilize local LPRs, we encourage you to reach out to coordinate data share

Cari N. Schieno | Program Analyst

DEASIL | National License Plate Reader Program (LPR)
El Paso Intelligence Center (EPIC)
Desk: (571) 387-4220 | Cell: (915) [redacted]
Cari.N.Schieno@usdoj.gov

"Do right and fear not"

"We'd love to hear any success stories from you, the users. These justify the coverage and growth of this program!"
You can send your stories to LPR@usdoj.gov or to cari.n.schieno@usdoj.gov
Password/Account reset LPR@usdoj.gov

From: Hersey, Kevin <KCHersey@DEA.USDOJ.GOV>
Sent: Tuesday, April 21, 2020 3:26 PM
To: LPR <LPR@dea.usdoj.gov>
Subject: Re: SEAR-2020-03428 for Case #CZ-17-0025

Hi Cari-

Thank you for reaching out.
We did not utilize DEASIL, and I'm sorry to report that I have never been introduced to it.
In the current instance, a Mass State Police Trooper (TFO) entered our target vehicle into the LPR system in MA on our behalf and further alerted me to the notification.
I am interested in learning more about DEASIL and I will research it further.

Best regards,

Kevin Hersey
DEA New England Field Division
New Bedford Resident Office
617-[redacted] (cell)

On Apr 21, 2020, at 3:22 PM, LPR <LPR@dea.usdoj.gov> wrote:

> Hello SA Tenore and SA Hersey:
>
> I wanted to congratulate you on your recent successful mission! I am contacting you on behalf of the LPR program and I wondered, at your convenience, if you could confirm if you utilized DEASIL? If you did, would you be willing to share with us any additional information (I.E. seizure images and/or LPR hit) for DEASIL publications/training materials?

We greatly appreciate any and all input!
V/r

Cari N. Schieno | Program Analyst

DEASIL | National License Plate Reader Program (LPR)
El Paso Intelligence Center (EPIC)
Desk: (571) 387-4220 | Cell: (915) [redacted]
Cari.N.Schieno@usdoj.gov

"Do right and fear not"

"We'd love to hear any success stories from you, the users. These justify the coverage and growth of this program!"
You can send your stories to LPR@usdoj.gov or to cari.n.schieno@usdoj.gov
Password/Account reset LPR@usdoj.gov

From: Concorde_Notification_Service <Concorde_Notification_Service@dea.usdoj.gov>
Sent: Tuesday, April 21, 2020 10:25 AM
To: SEAR-New England <SEAR-NewEngland@dea.usdoj.gov>; CommandCenter-SEARS <CCSears@dea.usdoj.gov>; DEA.ONSI <DEAONSI@dea.usdoj.gov>; EPIC Bulk Currency SEARS Mailbox <EPIC.BulkCurrency.Se@dea.usdoj.gov>; NCWSEARS <NCWSEARS@dea.usdoj.gov>; ST - Emerging Technologies Support <TWG@dea.usdoj.gov>; SEAR-HQ <SEAR-HQ@dea.usdoj.gov>; DeLena, Jon C. <JCDeLena@DEA.USDOJ.GOV>; Bonner, Richard B. <rbbonner@dea.usdoj.gov>; Bonaventura Jr., Ronald <RBonaventura@dea.usdoj.gov>; Boyle, Brian D. <BDBoyle@DEA.USDOJ.GOV>; Belleau, Stephen P. <SPBelleau@dea.usdoj.gov>; Skeffington, Mark E. <MESkeffington@DEA.USDOJ.GOV>; Parrish, Lonnie L. <LLParrish@DEA.USDOJ.GOV>; Abraham Jr., Michael <MAbraham@dea.usdoj.gov>; Tenore, Louis (Jim) <LJTenore@DEA.USDOJ.GOV>; Desmond, Timothy <TJDesmond@DEA.USDOJ.GOV>; Morse, Asa C. <AXMorse@DEA.USDOJ.GOV>; Hersey, Kevin <KCHersey@DEA.USDOJ.GOV>; Angelucci, Albert P. <APAngelucci@DEA.USDOJ.GOV>; Lanzoni, David L. <DLLanzoni@DEA.USDOJ.GOV>; Krysil, Cara L <CLKrysil@dea.usdoj.gov>
Subject: SEAR-2020-03428 for Case #CZ-17-0025

Significant Enforcement Activity Report for Case #CZ-17-0025

SEAR Number: SEAR-2020-03428
Date of Submission: 4/21/2020
DEA Division: New England Field Division

From: Bender, Sean (POL)
To: Thibault, Amy (POL)
Cc: Smith, Eleanor (POL)
Subject: DRAFT - CFC Overview & Resources - NCO + LT Supervisor Training - January 2022
Date: Wednesday, December 29, 2021 10:04:00 AM
Attachments: DRAFT - Fusion Center Resources + Overview - DFS - SB.pptx
CFC Overview & Resources Training - Lesson Plan.docx

Good Morning, Amy -

Please find the attached *DRAFT - Fusion Center Overview & Resources (U//LES)* presentation and accompanying lesson plan, developed for the January/February 2022 Massachusetts State Police NCO + LT Supervisor Training(s), to be held on 1/4/2022, 1/11/2022, 1/25/2022, & 2/1/2022 at the Massachusetts State Police Academy (SPA) and/or Homeland Security Operations Center (HSOC).

For review, at your convenience.

It looks longer than it is at 28 slides, but it is very picture heavy and several slides are just contact information, etc. Rather than go in depth into each data source, I just want to be able to throw up a screenshot and describe in a couple sentences what information is available and maybe a couple hypothetical use cases. My objective is to give the class an awareness of what is *available to them* and how to request it, not make them experts.

1. Title Slide > Introduction > Contact Information > Hours of Operation
2. Workflow > Intake > Tactical Support (CFC Watch Center) + Strategic Support (CFC Maynard)
3. (U//LES) Disclaimer
4. CFC Mission Statement
5. Brief Overview of Fusion Centers (E.g. At least one in every state, CFC + BRIC in MA)
6. Overview of CFC Resources / Function
7. CJIS (Advanced Tools [Other than CJISWeb MSP 3.0])
8. CJIS > Brief Mention of AFIS-R
9. CJIS > Brief Mention of InmateWeb
10. CJIS > Brief Mention of InmateWeb (2nd Screenshot)
11. ACISS > Brief Mention of ACISS
12. Commercial Data Sources > CLEAR
13. Commercial Data Sources > TLO
14. Commercial Data Sources > ISO
15. Coplink > Brief Mention
16. ALPR > Brief Overview of Historical Data / Hotlists
17. OSINT > Brief Overview of OSINT Uses (Finding associates, etc)
18. Situational Awareness > SITREPS
19. Situational Awareness > Bulletins

20. PowerDMS > Intelligence Resources
21. Overview - SAR Indicators & Behaviors (1)
22. Overview - SAR Indicators & Behaviors (2)
23. Overview - SAR Indicators & Behaviors (3)
24. Special Event Support
25. INTERPOL
26. CCIP
27. MCP
28. Questions? > Contact Information (Again)

Let me know what you think? Once approved, I will forward Tpr. Paquette a copy of the signed Lesson Plan Cover Sheet for the Academy record.

Respectfully,

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

From: Terrey, Susan (EPS)
To: Staples, Jennifer (POL); Lord, Spencer (CDA)
Cc: Boyd, Donald A (EPS)
Subject: FW: 6/24 Joint Committee on Transportation - ALPR
Date: Friday, June 25, 2021 11:05:01 AM
Attachments: H.3597 & 3564 - Act Relative to License Plate Readers.docx
H.3609 – Act Relative to Unmanned Aerial Systems.docx

Jenn & Spence: Don a new member of our legal team attended the legislative hearing on the ALPR - see his notes below as well as his summaries of the bills. Let us know if you would like to discuss more.

From: Boyd, Donald A (EPS) <Donald.A.Boyd@mass.gov>
Sent: Friday, June 25, 2021 10:12 AM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: 6/24 Joint Committee on Transportation - ALPR

Good Morning!

The joint committee on transportation held a public hearing on ALPR regulations yesterday. Outlines for both ALPR bills along with the proposed Drone regulation are attached for reference. Highlights and comments of the hearing are listed below:

Public Comment

- Arline I. - Director of Mass. LGBTQI Political Group
    - Spoke in broad support of both ALPR bills
    - Expressed desire to regulate use of ALPR system to protect privacy of LGBTQI community so that an individual's movements are not specifically targeted by law enforcement for unlawful purposes (bias)
- ACLU
    - Spoke in support of H.3564
        - Less comprehensive bill of the two, does not create obligations specific to EPS as seen in H.3597
    - Believes **14 day data** retention cap is reasonable
    - Supports **warrant requirement** for law enforcement access to system
    - Reasoned that 16 states have adopted similar legislation including Maine and New Hampshire
        - ME ST T.29-A s. 2117-A
        - NH ST s. 261:75-b
- No comment by committee members
- No public or committee comment on H.3609 – Drone Regulation

Feel free to reach out with any follow-up questions!

-Don

From: Range, Scott (POL)
To: Kelley, David
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Friday, April 9, 2021 12:42:00 PM
Attachments: HIDTA_NCRIC CONOP MAY2020.docx
Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

From: Range, Scott (POL)
Sent: Monday, April 5, 2021 12:43 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, April 5, 2021 12:00 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law

enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is

accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle

information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do

so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From:	Range, Scott (POL)
To:	Range, Scott (POL)
Subject:	FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date:	Monday, April 5, 2021 12:43:00 PM
Attachments:	HIDTA_NCRIC CONOP MAY2020.docx Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, April 5, 2021 12:00 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are

inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From:	Range, Scott (POL)
To:	Bender, Sean (POL)
Subject:	FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date:	Monday, April 5, 2021 11:53:37 AM
Attachments:	Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.pdf HIDTA_NCRIC CONOP MAY2020 (1).pdf

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or

a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses

the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence.

In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the

appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From:	Quinn, Dermot (POL)
To:	Range, Scott (POL)
Subject:	FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date:	Monday, March 8, 2021 2:53:13 PM
Attachments:	Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.pdf HIDTA_NCRIC CONOP MAY2020 (1).pdf

---

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS

Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

-

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various

federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history

information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC

personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Fallon, Jay
To: Quinn, Dermot (POL)
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Monday, March 8, 2021 2:11:32 PM
Attachments: Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.pdf
HIDTA_NCRIC CONOP MAY2020 (1).pdf

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

-

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide

them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to

comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a

secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From:	Range, Scott (POL)
To:	Kelley, David
Subject:	FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date:	Friday, April 9, 2021 12:42:00 PM
Attachments:	HIDTA_NCRIC CONOP MAY2020.docx Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

From: Range, Scott (POL)
Sent: Monday, April 5, 2021 12:43 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, April 5, 2021 12:00 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law

enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is

accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle

information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do

so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Donovan, Gerald (POL)
To: POL-DL-ICAC; POL-DL-DEMS
Subject: Fw: Emailing: MDEG Second Version 062021
Date: Thursday, June 24, 2021 12:40:08 PM
Attachments: MDEG Second Version 062021.pdf

I might have missed this, but just in case no one else received it.

Respectfully,

Trooper Jerry Donovan, #3424
Massachusetts State Police
Cyber Crime Unit
Internet Crimes Against Children Task Force
50 Maple St, Milford, MA 01757
W: (774) 462-3750
Gerald.Donovan@pol.state.ma.us

From: Lavoie, Matt (CPI) <matt.lavoie@mass.gov>
Sent: Thursday, June 24, 2021 12:21 PM
To: Donovan, Gerald (POL) <gerald.donovan@pol.state.ma.us>
Subject: Emailing: MDEG Second Version 062021

Your message is ready to be sent with the following file or link attachments:

MDEG Second Version 062021

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

From: Wilcox, Christopher (POL)
To: Egnitz, Brian (POL)
Subject: FW: License Plate Reader Program Best Practices Guide.
Date: Friday, November 12, 2021 10:04:00 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

---

Brian – Some great stuff in here

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, November 12, 2021 9:11 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: License Plate Reader Program Best Practices Guide.

Sir,
Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From:	Wilcox, Christopher (POL)
To:	Pack, Noah (POL)
Subject:	FW: License Plate Reader Program Best Practices Guide.
Date:	Friday, November 12, 2021 9:38:00 AM
Attachments:	LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, November 12, 2021 9:11 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: License Plate Reader Program Best Practices Guide.

Sir,
Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From:	Wilcox, Christopher (POL)
To:	Scott, Michael (POL)
Subject:	FW: License Plate Reader Program Best Practices Guide.
Date:	Friday, November 12, 2021 10:04:00 AM
Attachments:	LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, November 12, 2021 9:11 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: License Plate Reader Program Best Practices Guide.

Sir,
Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From: Brooks, Brian (POL)
To: Bender, Sean (POL)
Subject: FW: LPR"s
Date: Tuesday, November 2, 2021 10:59:00 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
image002.png

From: Boyle, Christopher (DOT) <Christopher.P.Boyle@dot.state.ma.us>
Sent: Tuesday, November 2, 2021 10:49 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>
Subject: LPR's

Sirs,

AAMVA is the American Association of Motor Vehicle Administrators. It is a private organization that almost every RMV/DMV is part of.

They just released the License Plate Reader Program Best Practices Guide.

I have attached it if it can be of assistance.

Respectfully,

Chris

Lieutenant Christopher Boyle #2710
Massachusetts State Police
Division of Homeland Security and Preparedness
Fraud Identification Unit
185 Kneeland St., 5th Floor
Boston, MA 02111
christopher.boyle@mass.gov
cell: 781-[redacted]

From: Egnitz, Brian (POL)
To: Pack, Noah (POL)
Subject: FW: Massachusetts State Police ALPR - Verizon Mobile Private Network
Date: Monday, November 22, 2021 2:01:00 PM
Attachments: MSP- ALPR Private Network Options 03 01 2021.pdf

---

From: Jussaume, Carolyn B <carolyn.jussaume@verizonwireless.com>
Sent: Monday, March 1, 2021 9:34 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Michael Caralis <michael.caralis@verizonwireless.com>; Paul Ralston <paul.ralston@verizonwireless.com>; Marshall Roger <roger.marshall@verizonwireless.com>; William M Reed <william.reed1@one.verizon.com>; Nugent, Michael (Data Sales) <michael.nugent@verizonwireless.com>; Borell, Ben <Ben.Borell@verizonwireless.com>
Subject: Re: Massachusetts State Police ALPR - Verizon Mobile Private Network

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

Lt Colonel Quinn and Brian

Attached is a high level summary of each option with the associated costs from Verizon. Pls also check out the documents that Ben provided, as they provide a more thorough private network explanation. We did make some assumptions about the amount of bandwidth needed for the Secure Cloud Interconnect option not really knowing the projected data needs at this point (this can be fine tuned once more information is available). As we mentioned, Verizon does have professional services which can assist in many areas- if there are some areas that MSP would like assistance, pls let us know and we can put together a statement of work and a quote for that as well.

Please let us know if you would like to set up some time to review the information.

Carolyn

On Thu, Feb 25, 2021 at 10:27 AM Borell, Benjamin <ben.borell@verizonwireless.com> wrote:

> Good Morning,
>
> Following up on our conversation from the other day, attached are a few documents:
>
> - A Verizon Mobile Private Network (MPN) whitepaper
> - A PDF diagram of proposed design options for LTE routers to reach AWS
> - A Word document that would be used to collect customer network inputs for an MPN using IPSec VPN over the Internet.

- I have highlighted some key sections of the form and have also made some notes in *Comic Sans* font to clarify what VZ is seeking in that particular section.
- If the decision is reached by MSP to utilize Secure Cloud Interconnect I would provide a similar, but slightly different form which does not require inputs for VPN tunnels.

We'd be happy to set up a web call to review one or both private network intake forms. I will defer to Carolyn, Paul, and William to provide pricing for the two design options.

Lastly, both design options are supported by the Verizon Wireless Help Desk (WEHD) which offers 24x7x365 tier two tech support for Mobile Private Network projects.

Thank you,
Ben



Benjamin Borell

Sr. Solutions Engineer
Field Pre-Sales Engineering
Verizon Business Group

M 617 872 8330

--



Carolyn Jussaume

Business Development
Massachusetts Government Team
Verizon Business Group

M 617 699 3900
1 Washington Mall, 6th Floor
Boston, Massachusetts 02109



From: Pack, Noah (POL)
Subject: Fw: MOU Contacts
Date: Wednesday, December 15, 2021 9:48:00 AM
Attachments: image001.png
image002.png
image003.png
BCPO+Law+Enforcement+Directive+No.+2020-10+with+Attachments.pdf
Post Falls Idaho PD ALPR MOU-04202021.pdf

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, December 14, 2021 2:47 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: MOU Contacts

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

Great,

I've been waiting on some customers for MOU's that you had asked for. Not to delay any further I've attached two that I've received so far for your review.

For contacts: John Mittmann -IT Administrator jmittmann@postfallspolice.com; (208) 773-3517 of Post Falls Police and Brian Rodriques -Asst Deputy Director brodriques@ncric.ca.gov; (415) 710-9702 of The Northern California Regional Intelligence Center are fairly large user of ours.

Regards,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, December 14, 2021 10:58 AM
To: John Tedona <jtedona@neology.net>
Subject: Re: Wednesday 1PM Meeting

Hi John,

That's fine with me. There is a TV available in our conference room.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Monday, December 13, 2021 9:56 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Wednesday 1PM Meeting

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

Hi Noah,

I'd like to have Bob Fecteau and Kory Koster of BCM Controls join us in Wednesday's meeting if that's okay with you. This way you will have representation of the manufacture (me), the sales side (Bob Fecteau) and the on-site support technician (Kory Koster) in the meeting to cover any questions that you may have.

I'll have my ALPR demonstration vehicle so I can provide a live mobile ALPR demo. To provide an overview of BOSS4 will a large monitor be available that I could connect with my laptop for easier viewing?

Thanks,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

From:	Wilcox, Christopher (POL)
To:	Warren, Rosemary (POL)
Subject:	FW: postings
Date:	Friday, September 10, 2021 9:57:00 AM
Attachments:	National_ANPR_Service_technical_specifications.pdf National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version) - GOV.UK.pdf NASPLE_Version_2.1_November_2020.pdf

---

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, September 9, 2021 5:51 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: RE: postings

Here are a bunch of ideas for your consideration. Let me know when you can review and I can add context. It's a mix of tasks that would need to be simplified for a posting. I've also included some good docs that we could borrow from.

-Brian

ALPR coordinator will:

- Work to establish a new MSP ALPR Program
- facilitate ALPR data sharing thought public safety in the public safety community
- Manage MSP Commercial ALPR Vendor accounts, such as Vigilant National plate reader database, or new systems offered to MSP like Flock
- Track trends in ALPR technology
- Track legal rulings and advise
- Maintain a list of known ALPR systems used by Public Safety (including Department, system type, technology used, retention period and contacts)
- Provide support to MSP and Local Departments in use or purchase of ALPR technology as requested
- Facilitate sharing of Hotlists to disparate systems for Amber or related significant events
- Maintain hotlist compliance (Case number, cause and removal in timely manner)
- Perform advanced ALPR searches (such as convoy or cohort)
- Maintain Regional Hotlist / WMS Alert system
- Become POC for MassTurn Pike exigency requests (not sure who does this now)
- Establish a ALPR minimum data standard for new Equipment
- Administer the Agency ALPR system
- Perform system and hotlist audits
- Monitor system and report issues or outages to appropriate personnel
- Manage user accounts and permissions
- Interact with ALPR vendor(s)
- Identify best practices
- Provide user training
- Provide expert witness testimony

- Maintain success stores
- Monitor cloud subscription for overages
- Perform ad-hoc and statistical reporting
- Respond to legal process and public record requests
- Work with MSP / EOPSS Legal to create data sharing agreements with contributing agencies.
    - To Include data standards and audit requirements for all submitting Agencies
- Work with MSP / EOPSS Legal to execute cloud agreement with MSP ALPR vendor [Neology] (see DCJIS template)
- Work with MSP / EOPSS Legal to execute agreement with 3rd party ALPR vendors (such as Flock or Vigilant)
- Seek grants for replacing equipment
- Work with Fiscal to budget for replacement equipment
- Coordinate new ALPR camera purchases, such as the Truck Teams new purchase to maintain compliant equipment
- Work with TSS/EOPSS/MSP to migrate preserved data
- Work with TSS/EOPSS/MSP to migrate existing cameras to the new Cloud solution
- Work with TSS/EOPSS/MSP to migrate hot file connections to cloud
- Work with TSS/EOPSS/MSP to migrate decommission EOPSS BOSS 3.6

Desired experience

- Existing subject matter expert in ALPR technology
- Experience in use of or application of ALPR technology
- Proficient in use of web based technologies
- Experience in managing applications and permissions

From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Sent: Thursday, September 9, 2021 12:41 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: postings

Brian - Can you get me a couple of bullets for LPR Coordinator?

Lieutenant Colonel Christopher T. Wilcox

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Road

Framingham, MA 01702

From: Wilcox, Christopher (POL)
To: Warren, Rosemary (POL)
Subject: Fw: postings
Date: Wednesday, November 10, 2021 3:27:40 PM
Attachments: ALPR Coordinator Posting - Sergeant - September 2021.docx

---

Lieutenant Colonel Christopher T. Wilcox
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road
Framingham, MA 01702

508 820-7301

From: Wilcox, Christopher (POL)
Sent: Friday, September 10, 2021 11:42 AM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Subject: FW: postings

From: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Sent: Friday, September 10, 2021 11:20 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: RE: postings

LTC,

Please take a look at this first DRAFT

Respectfully,

Rose

Rosemary J. Warren
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Office: 508-988-7310
Rosemary.Warren@mass.gov

From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Sent: Friday, September 10, 2021 9:57 AM
To: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Subject: FW: postings

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, September 9, 2021 5:51 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: RE: postings

Here are a bunch of ideas for your consideration. Let me know when you can review and I can add context. It's a mix of tasks that would need to be simplified for a posting. I've also included some good docs that we could borrow from.

-Brian

ALPR coordinator will:

- Work to establish a new MSP ALPR Program
- facilitate ALPR data sharing thought public safety in the public safety community
- Manage MSP Commercial ALPR Vendor accounts, such as Vigilant National plate reader database, or new systems offered to MSP like Flock
- Track trends in ALPR technology
- Track legal rulings and advise
- Maintain a list of known ALPR systems used by Public Safety (including Department, system type, technology used, retention period and contacts)
- Provide support to MSP and Local Departments in use or purchase of ALPR technology as requested
- Facilitate sharing of Hotlists to disparate systems for Amber or related significant events
- Maintain hotlist compliance (Case number, cause and removal in timely manner)
- Perform advanced ALPR searches (such as convoy or cohort)
- Maintain Regional Hotlist / WMS Alert system
- Become POC for MassTurn Pike exigency requests (not sure who does this now)
- Establish a ALPR minimum data standard for new Equipment
- Administer the Agency ALPR system
- Perform system and hotlist audits
- Monitor system and report issues or outages to appropriate personnel
- Manage user accounts and permissions
- Interact with ALPR vendor(s)
- Identify best practices
- Provide user training
- Provide expert witness testimony
- Maintain success stores
- Monitor cloud subscription for overages
- Perform ad-hoc and statistical reporting
- Respond to legal process and public record requests
- Work with MSP / EOPSS Legal to create data sharing agreements with contributing agencies.

    - To Include data standards and audit requirements for all submitting Agencies
- Work with MSP / EOPSS Legal to execute cloud agreement with MSP ALPR vendor [Neology] (see DCJIS template)
- Work with MSP / EOPSS Legal to execute agreement with 3rd party ALPR vendors (such as Flock or Vigilant)
- Seek grants for replacing equipment
- Work with Fiscal to budget for replacement equipment
- Coordinate new ALPR camera purchases, such as the Truck Teams new purchase to maintain compliant equipment
- Work with TSS/EOPSS/MSP to migrate preserved data
- Work with TSS/EOPSS/MSP to migrate existing cameras to the new Cloud solution
- Work with TSS/EOPSS/MSP to migrate hot file connections to cloud
- Work with TSS/EOPSS/MSP to migrate decommission EOPSS BOSS 3.6

Desired experience

- Existing subject matter expert in ALPR technology
- Experience in use of or application of ALPR technology
- Proficient in use of web based technologies
- Experience in managing applications and permissions

From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Sent: Thursday, September 9, 2021 12:41 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: postings

Brian - Can you get me a couple of bullets for LPR Coordinator?

Lieutenant Colonel Christopher T. Wilcox
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road
Framingham, MA 01702

508 820-7301

From: Bender, Sean (POL)
To: Thibault, Amy (POL)
Subject: Fw: Promulgation of 19-SO-12
Date: Thursday, March 18, 2021 7:44:43 AM
Attachments: 19-SO-12 Distribution of General Order.pdf
TRF-11 Automatic License Plate Recognition Revised 10-1-2019 with highlights.pdf

---

Applicable RE: Vigilant?

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

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, November 12, 2019 10:47 AM
To: McCarthy, Daniel (POL) <Daniel.McCarthy@pol.state.ma.us>
Cc: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: Fw: Promulgation of 19-SO-12

From: Strategic Planning (POL) <strategic.planning@massgov.onmicrosoft.com>
Sent: Tuesday, October 1, 2019 5:20 PM
To: POL-DL-All Users <POL-DL-AllUsers@MassMail.State.MA.US>
Subject: Promulgation of 19-SO-12

Please be advised that the following Special Order has been promulgated:

- **19-SO-12 Distribution of General Order**
  TRF-11 Automatic License Plate Recognition

Please also be advised that the official General Order listed in the above Special Order has been promulgated.

Strategic Planning Section
470 Worcester Road
Framingham, Massachusetts 01702

From: Fitzge a d Thomas (POL)
Subject: Fw: Proposed Reg/Statute updates to c. 90 or FAST Act compl ance
Date: Monday April 5 2021 4:18:10 PM
Attachments: 00 CMR 7 Redl ne.doc
Redl ne to c 90 Sect on 1 - de init ons.doc
Redl ne to c 90 Sect on 19A.doc
Redl ne to G L c 90 Section 19 .doc
Redl ne to G L c 90 Section 19F.doc
RE Pro osed Dates to c 90 or FAST Act com l ance.msg

From Osborne Chester (DOT) <Chester.Osborne@dot state.ma.us>
Sent Monday April 5 2021 15 22
To Myslinski Tara (DOT)
Cc DelVento Anthony J. (DOT) Fanning Jessica M. (DOT) Fitzgerald Thomas (POL) Rizzuto Elizabeth (DOT) N les Makaela (DOT) Lee Donna M. (DOT) Weidele Matthew (DOT) Bardow Alexander K. (DOT) Slack Just n (DOT)
Subject FW Proposed Reg/Statute updates to c. 90 for FAST Act compliance

Hello all. As many of you know Ms. Myslinski has been working hard to updated the regs around commercial ehicles and frieght. These latest drafts (a tached) represent he culmination of many months of work drafts and re isions to support this line of effort. We now find oursel es at the last draft and facing the deadline to mo e th s up the chain.

Please take some time to re iew the attached and below prior o Thursday of his week. If you need to make edits please use track changes in the doc and rename it wi h your stakeholder group in the file name and send it back to Ms. Myslinski and CC myself no later than COB Thursday 8 h. If you ha e no comments or edits and affirmation of same is appreciated.

In a moment I w ll send a calendar in ite for 11am Thursday the 8th this is by no means a mandatory mee ing for anyone in fact it is really more of "office hours" in case you need to ha e a con ersation around any feedback and to conduct any joint editing exercises.

When making re iew please consider any limitations for the MHS Tunnels Bridges or other unique situations. As well as inform as to any other rules policies or procedures that these proposed changes could impact. Last feel free to include any stakeholders or members of your team that I may ha e missed. Thank you for your support in his matter.
V/r Chet.

Ches er Osborne
Dir. of TSMO
617.719 5 77

From Myslinski Tara (DOT) <Tara.Myslinski@dot state.ma.us>
Sent Monday April 5 2021 2 57 PM
To Osborne Ches er (DOT) <Chester.Osborne@dot.state.ma.us>
Cc Fenton Eileen (DOT) <Eileen.Fenton@dot.state.ma us>
Subject Proposed Reg/Statute updates to c. 90 for FAST Act compliance
Importance High

Chet the attached redlines of current sta utes and regs are ready for re iew by the FOG. I added a couple of items based on Chris's feedback. You may also want o send the FOG Chris's email and/or the link to the FAST Act pro isions that Chris sent (attached and below for con enience) unless you hink that would confuse the re ew – hat is up to you.

ht ps://ops fhwa.dot.go freight/pol plng finance/policy/fas act/twopro isions/index.htm#description<https://urldefense.com/ 3/ https /ops.fhwa do go /freight/pol plng finance/pol cy fastact/twopro isions/index.htm*description Iw!!CUhgOOZqV7M!3V0RGH1tjCKZFl xErsVE0Rif1qU5JjzdnpKrfcCo 1JgMnkK3PsDhGiD7wjFxQXKmUNCk$>

If we are going to submit these legislati e changes as part of he Go ernor's safety bill we need the language by April 12 – a week from today. Do you th nk we could get comments this week? Happy to meet and discuss.

Tara Myslinski
Senior Lead Counsel Regulatory & Compliance
MassDOT
Ten Park Plaza Suite 3510
Boston Massachuse ts 02116
Mobile 857-360-6810
Tara.myslinsk @dot state.ma.us<mailto:T y l @ >

[image003]

MassDOT and the MBTA are subject to MGL Chpt.66 Sec.10 Public Records Law. Email sent or recei ed by MassDOT and MBTA employees are subject to these laws. Unless otherw se exempted from the public records law senders and recei ers of MassDOT and MBTA email should presume that the email are sub ect to release upon request and to state record retention requirements.

Conf dentiality No ice [This communication (includ ng any attachments) is only intended for the user of the indi idual or entity to which t is directed. It may conta n information that is pri ileged confidential and exempt from disclosure under applicable law and should not be read cop ed or o herwise used by any other person. If recei ed in error please notify he sender immediately and delete the e-mail and any attachment(s) from your system without copying forwarding disclos ng or using it n any other way.

From: Lavoie, Matt (CPI)
To: Barnard, Diana (CPI); Cosgrove, Richard (CPI); Diotte, Jeffrey (POL); Dunphy, David (POL); Fries, Joshua (POL); Furtado, Gregory (POL); Hanafin, John (CPI); Lavoie, Matt (CPI); Macdonald, Paul (POL); McCabe, Scott (CPI); Perkins, Taylor (CPI); Porter, Bradford (POL); Powell, Marc S (POL); Shaw, Dustin (POL); Ungechauer, Stan J (POL); Gregg, Theodore (POL); Walczak, David J (POL); Waskiewicz, Justin J (POL)
Subject: FW: The Massachusetts Digital Evidence Guide June 2021
Date: Wednesday, June 16, 2021 3:33:25 PM
Attachments: MDEG Second Version 062021.pdf

Attached is the updated Digital Evidence guide put out by the AG's office. It covers the search and seizer of pretty much any type of digital evidence and should answer any questions on search warrant issues. I also saved it on the Q-Drive under CSLI-Ping folder.

Sergeant Matthew R. Lavoie #3138
Massachusetts State Police Detetive Unit
Cape Cod & the Islands
Office: (508) 790-5799

-----Original Message-----
From: mdec@listserv riss net <mdec@listserv.riss net>
Sent: Tuesday, June 1, 2021 4:34 PM
To: mdec@listserv.riss.net
Subject: The Massachusetts Digital Evidence Guide June 2021

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

Good Afternoon Everyone,

Attached, please find the second version of the Massachusetts Digital Evidence Guide, June 2021 edition. It is updated with cases issued through early this year. The MDEG first edition was issued in June of 2015, a resource and vision of the Cyber Crime Division of the AGO, and particularly CCD Chief Tom Ralph, who now serves as Chief of the Middlesex Appeals Division and active MDEC Member. The first edition was cited to in more than one decision from Massachusetts courts, including the SJC in the 2017 case Commonwealth v. Molina. In Molina, the SJC stated, "The Attorney General's existing digital evidence guide offers helpful parameters, and we invite the Attorney General to develop further guidance for the conduct of digital searches that could be made available to both State and local officers conducting digital searches." In short, this MDEG has proved to be an invaluable resource for many over the course of the years. One of the ways we have continued to address this specific concern from the SJC are the continued training and outreach initiatives of MDEC.

Starting with Dorelas in 2016, our Appeals Courts have issued dozens of impact cases on digital evidence. So many in fact that keeping up with updates to the MDEG has been very difficult. Remarkably enough, we already have several cases to add since the attached version was finalized. Regardless, it is here. Many of you helped contribute thoughts and submissions a few years ago. Lots of legal interns - and a partnership with the AGO Appeals Division - helped push it over the finish line. Thank you to all, including AGO Appeals Division Chief Randy Ravitz and Deputy Division Chief Tom Bocian and AAsG Maria Granik and Anna Lumelsky, for the contributions of time, effort, and expertise to this important initiative.

Please email me with any questions or if you notice anything that needs to be adjusted. We have stared at this endlessly for long periods of time. Mark Twain wisely said, "continued progress is better than delayed perfection." So this resource will continue to be a work in progress. Every police officer and prosecutor in Massachusetts can

benefit from the time investment.

-CK

_____

Christopher W. Kelly
Director
Digital Evidence Laboratory
Commonwealth of Massachusetts
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
617.963.2146 (office)
617.963.2620 (lab main)
christopher kelly@mass.gov

This e-mail, including attachments, may contain confidential or privileged information and is solely for the use of the intended recipient. If you have received this communication in error, please notify the sender immediately and delete this message from your system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

##############################
This message is sent to you because you are subscribed to the mailing list mdec@listserv.riss.net.
To unsubscribe, E-mail to: mdec-off@listserv.riss.net

Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, forwarding or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Any information that is disseminated via listserv riss net is considered property of the issuing agency.

From: Craig Lynch
To: Pack, Noah (POL)
Subject: Fwd: MOU and Axon Promo - Flock Safety
Date: Tuesday, December 7, 2021 9:51:10 PM
Attachments: NPF LPR Study Brief_11-15-2021.pdf

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

Sgt - Please see the response below and the attachment. Do you have some time to talk this week?

Craig

---------- Forwarded message ---------
From: **Bob Carter** <bob.carter@flocksafety.com>
Date: Tue, Dec 7, 2021 at 9:38 PM
Subject: Re: MOU and Axon Promo - Flock Safety
To: Craig Lynch <craig.lynch@flocksafety.com>

The LPR database is controlled and owned by the PD. NPF will not have access to this. The data is statistical analysis. The attached document provides more information. Please set up a call with the three of us to discuss.

Bob Carter
Director, Strategic Alliances
Flock Safety
404-631-6317 | bob.carter@flocksafety.com

On Tue, Dec 7, 2021 at 9:33 PM Craig Lynch <craig.lynch@flocksafety.com> wrote:

> Mr Bob - Mass State Police is interested in the Axon free cams . Any insight on the email below?
>
> ---------- Forwarded message ---------
> From: **Pack, Noah (POL)** <noah.pack@state.ma.us>
> Date: Tue, Dec 7, 2021 at 9:04 PM
> Subject: Re: MOU and Axon Promo - Flock Safety
> To: Craig Lynch <craig.lynch@flocksafety.com>
>
> Hi Craig,
>
> I am setting up a meeting with our legal section regarding a number of issues, to include the Flock MOU and nationwide study/trial program. I expect to be asked for the fine print on the

study, including what are we expected to do with our participation, what happens to the data, etc. Can you provide any further info on that?

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: Craig Lynch <craig.lynch@flocksafety.com>
Sent: Wednesday, December 1, 2021 9:16 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: MOU and Axon Promo - Flock Safety

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

Sgt Pack - Nice speaking with you this morning. I have attached the Flock Safety MOU which will give access to everything in the system as a paying custom other than the NationWide Search of ~9500 cameras.

Below is the email with details on the Axon promotion. It's a bit lengthy, but 1 year, no obligation, no multi-year commitment.

As Axon Founder and CEO Rick Smith announced at the MCSA Fall Meeting, Axon along with its partner Flock Safety, will provide all MCSA agencies Automated License Plate Readers (ALPR) for one year for those willing to participate in a national study conducted by the Police Foundation. While many recognize the crime-reduction benefits of ALPR technology, questions have been raised about how effective they are at reducing all crime types as well the civil liberties and privacy implications of this technology. This study will attempt to provide a robust research design and methodology to address those questions and concerns.

If your agency is willing to take part in this national study, you will receive:

- **25 Flock Safety ALPRs for 1 year, which includes the ALPR readers, solar or DC power, mounting equipment, and installation.**
- **This also includes all cloud hosting and analytics, including LTE connectivity,**

unlimited licenses, hotlist integration and alerts, and ongoing software enhancements.

- **Flock Safety will make their SMEs available to assist agencies with identifying the most effective ALPR locations.**
- **Agencies can purchase additional cameras beyond the 25. Axon and Flock will cover the installation costs of these additional cameras.**
- **This offer applies to any MCSA agency, including those that have already purchased Flock ALPRs.**
- **After the 1-year field trial offer ends, each agency has the option to purchase the units at $2500 per year per ALPR.**
- **Should an agency choose not to retain the ALPRs after the field trial, we will ensure that the agency is able to transfer their data to another system and we will remove the ALPRs at no cost to the agency.**

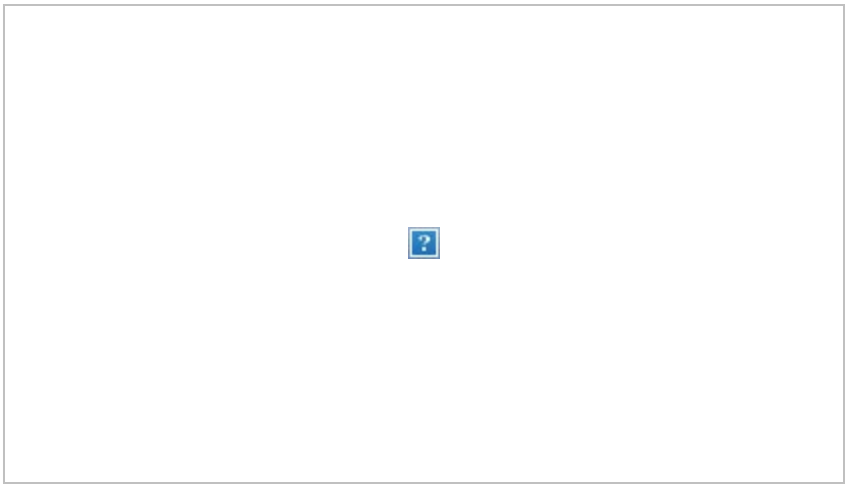
In addition, we understand that across the country there are varying laws and regulations about ALPR technology. Axon's Government Affairs team will be available to your agency to provide an overview of any state and county ALPR laws that are applicable. We will also provide model ALPR policies to your agency prior to deployment. And, our Government Affairs team can act as a resource to meet with and educate any county board member(s) on Axon, Flock Safety, ALPR technology — and our ethics-first design philosophy.

If you or your team have any questions, please let me know.

Thanks for your partnership,

Craig

--



This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s).

From: Cyr, Mark (POL)
To: Wilcox, Christopher (POL)
Subject: License Plate Reader Program Best Practices Guide.
Date: Friday, November 12, 2021 9:10:40 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

---

Sir,

Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From: Wilcox, Christopher (POL)
To: Benincasa, Jeanne (EPS)
Subject: LPR Article
Date: Friday, December 3, 2021 10:01:00 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

---

Undersecretary Benincasa – I attached a document about best practices for LPR Programs. It's very informative, and I felt Chapter 7 "LPR Success stories" was interesting. CTW

Lieutenant Colonel Christopher T. Wilcox
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road
Framingham, MA 01702

508 820-7301

From: Boyle, Christopher (DOT)
To: Cyr, Mark (POL); Tucker, Daniel T (POL); Brooks, Brian (POL); O"Hara, Edward (POL)
Subject: LPR"s
Date: Tuesday, November 2, 2021 10:48:35 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
image002.png

Sirs,

AAMVA is the American Association of Motor Vehicle Administrators. It is a private organization that almost every RMV/DMV is part of.

They just released the License Plate Reader Program Best Practices Guide.

I have attached it if it can be of assistance.

Respectfully,

Chris

Lieutenant Christopher Boyle #2710
Massachusetts State Police
Division of Homeland Security and Preparedness
Fraud Identification Unit
185 Kneeland St., 5th Floor
Boston, MA 02111
christopher.boyle@mass.gov
cell: 781-[redacted] G.L. c. 4 sec. 7 cl.26 (n)(s

To:	Wilcox, Christopher (POL)
Cc:	Egnitz, Brian (POL)
Date:	Monday, November 22, 2021 2:41:05 PM
Attachments:	MSP- ALPR Private Network Options 03 01 2021.pdf Pricing Proposal- BCM Controls_Sierra MP70 Routers, Accessories & ALMS Through June 30, 2022 REV1 10012021.pdf Pricing Proposal- BCM Controls_Sierra MP70 Routers, Accessories & ALMS Through June 30, 2023 REV1 10012021.pdf

---

Lieutenant Colonel Wilcox,

Please see the attached TFL and cost proposals for equipment and services that are necessary for the upgrade and maintenance of the Department's ALPR network.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona
To: Pack, Noah (POL)
Subject: Mobile Training
Date: Friday, December 10, 2021 11:57:19 AM
Attachments: image001.png
image002.png
image003.png
PAGIS 2.14 MANUAL_ADMIN.pdf
PAGIS 2.14 MANUAL_USERS.pdf

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

Noah,

I've attached the latest training PDFs for our mobile ALPR systems. A new version will be available soon that will include the NTP time server lock water mark on the vehicle over view and license plate images.

Regards,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Craig Lynch
To: Pack, Noah (POL)
Subject: MOU and Axon Promo - Flock Safety
Date: Wednesday, December 1, 2021 9:17:13 AM
Attachments: MA Massachusetts State PD - MOU.pdf

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

Sgt Pack - Nice speaking with you this morning. I have attached the Flock Safety MOU which will give access to everything in the system as a paying custom other than the NationWide Search of ~9500 cameras.

Below is the email with details on the Axon promotion. It's a bit lengthy, but 1 year, no obligation, no multi-year commitment.

As Axon Founder and CEO Rick Smith announced at the MCSA Fall Meeting, Axon along with its partner Flock Safety, will provide all MCSA agencies Automated License Plate Readers (ALPR) for one year for those willing to participate in a national study conducted by the Police Foundation. While many recognize the crime-reduction benefits of ALPR technology, questions have been raised about how effective they are at reducing all crime types as well the civil liberties and privacy implications of this technology. This study will attempt to provide a robust research design and methodology to address those questions and concerns.

If your agency is willing to take part in this national study, you will receive:

- **25 Flock Safety ALPRs for 1 year, which includes the ALPR readers, solar or DC power, mounting equipment, and installation.**
- **This also includes all cloud hosting and analytics, including LTE connectivity, unlimited licenses, hotlist integration and alerts, and ongoing software enhancements.**
- **Flock Safety will make their SMEs available to assist agencies with identifying the most effective ALPR locations.**
- **Agencies can purchase additional cameras beyond the 25. Axon and Flock will cover the installation costs of these additional cameras.**
- **This offer applies to any MCSA agency, including those that have already purchased Flock ALPRs.**
- **After the 1-year field trial offer ends, each agency has the option to purchase the units at $2500 per year per ALPR.**
- **Should an agency choose not to retain the ALPRs after the field trial, we will ensure that the agency is able to transfer their data to another system and we will remove the ALPRs at no cost to the agency.**

In addition, we understand that across the country there are varying laws and regulations about ALPR technology. Axon's Government Affairs team will be available to your agency to provide an overview of any state and county ALPR laws that are applicable. We will also provide model ALPR policies to your agency prior to deployment. And, our Government

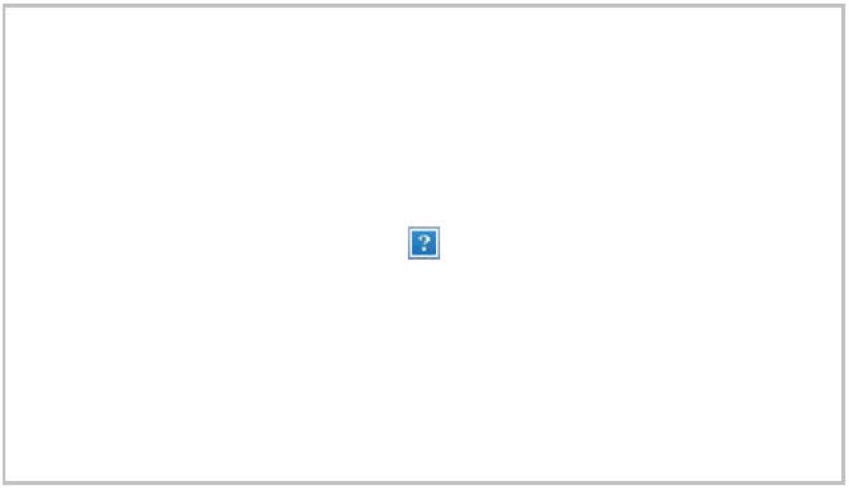
Affairs team can act as a resource to meet with and educate any county board member(s) on Axon, Flock Safety, ALPR technology — and our ethics-first design philosophy.

If you or your team have any questions, please let me know.

Thanks for your partnership,

Craig

--



From: John Tedona
To: Pack, Noah (POL)
Subject: MOU Contacts
Date: Tuesday, December 14, 2021 2:49:00 PM
Attachments: image001.png
image002.png
image003.png
BCPO+Law+Enforcement+Directive+No.+2020-10+with+Attachments.pdf
Post Falls Idaho PD ALPR MOU-04202021.pdf

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

Great,

I've been waiting on some customers for MOU's that you had asked for. Not to delay any further I've attached two that I've received so far for your review.

For contacts: John Mittmann -IT Administrator jmittmann@postfallspolice.com; (208) 773-3517 of Post Falls Police and Brian Rodriques -Asst Deputy Director brodriques@ncric.ca.gov; (415) 710-9702 of The Northern California Regional Intelligence Center are fairly large user of ours.

Regards,

neology
mobility [re]imagined

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, December 14, 2021 10:58 AM
To: John Tedona <jtedona@neology.net>
Subject: Re: Wednesday 1PM Meeting

Hi John,

That's fine with me. There is a TV available in our conference room.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Monday, December 13, 2021 9:56 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Wednesday 1PM Meeting

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

Hi Noah,

I'd like to have Bob Fecteau and Kory Koster of BCM Controls join us in Wednesday's meeting if that's okay with you. This way you will have representation of the manufacture (me), the sales side (Bob Fecteau) and the on-site support technician (Kory Koster) in the meeting to cover any questions that you may have.

I'll have my ALPR demonstration vehicle so I can provide a live mobile ALPR demo. To provide an overview of BOSS4 will a large monitor be available that I could connect with my laptop for easier viewing?

Thanks,



John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net



***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

From: Enrique Cramer
To: Sharon Easley (seasley@e-squared.org)
Cc: Fitzgerald, Thomas (POL)
Subject: MSP Smart Roadside Trailer - Extended Support & Maintenance Services
Date: Friday, October 1, 2021 12:23:27 PM
Attachments: Q2021851_MA_SP_IIS_Support_Maintenance_Services_(SMS)_Plan_Oct_1_2021.pdf

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

Hi Sharon,

As per our recent call, the extended support & maintenance services (SMS) for MA State Police Smartroadside Trailer expired yesterday.
Lt. Fitzgerald confirmed that they would like to extend SMS thus here is a quote for the next 3 years.

FYI – Previously, SMS for the trailer flowed through "Access Control Systems, Inc" who have a statewide contract with MSP. Moving forward, SMS will go directly through IIS.
Let me know if we need to do anything on our end (i.e. register as a vendor) to support this.

Cheers,

Enrique
778.384.4341

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series Today at 1:00 pm EST: CODY Systems
Date: Wednesday, May 12, 2021 9:16:55 AM
Attachments: May Calendar.pdf

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

Today's Sponsor Education Series presentation is hosted CODY Systems. Session information and a registration link are below. Also attached is the May Sponsor Education Series calendar.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data fusion technology fuels fusion centers with a one-stop search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider.

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Thank you for participating in the NFCA Sponsor Education Series.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series Today at 1:00 pm EST: CODY Systems
Date: Wednesday, May 12, 2021 9:11:06 AM
Attachments: May Calendar.pdf

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

Today's Sponsor Education Series presentation is hosted CODY Systems. Session information and a registration link are below. Also attached is the May Sponsor Education Series calendar.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data fusion technology fuels fusion centers with a one-stop search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider.

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Thank you for participating in the NFCA Sponsor Education Series.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series - May Calendar with Updated Links
Date: Tuesday, May 11, 2021 11:52:47 AM
Attachments: May Calendar.pdf

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

Good morning,

An update to the May NFCA Sponsor Education Series is attached. Several revised links are provided.

The Sponsor Education Series kicks off tomorrow (Wednesday, May 11) at 1:00 pm EST with a 30 minute webinar presented by CODY Systems. Information is below.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Please direct questions to Laura Milford at lmilford@nfcausa.org or 858-602-6050.

Thank you for participating in the NFCA Sponsor Education Series.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series - May Calendar
Date: Saturday, May 8, 2021 4:24:41 PM
Attachments: May Calendar.pdf

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

The National Fusion Center Association (NFCA) announces the launch of its 2020 Sponsor Education Series. The Series is a monthly calendar of webinars presented by our valued NFCA sponsors to educate and inform the fusion center community about evolving technologies and services relevant to the fusion center mission.

Sessions are scheduled for Tuesday, Wednesday and Thursday afternoons at 1:00 pm EST for 30 or 60 minutes.

The Sponsor Education Series schedule with session descriptions for May is attached. Please take a look and calendar time to attend sessions of interest to you.

If you have questions or need assistance, please contact Laura Milford, NFCA's sponsor liaison, at lmilford@nfcausa.org or 858-602-6050.

Thank you for your participation.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series Today at 1:00 pm EST: CODY Systems
Date: Wednesday, May 12, 2021 9:17:14 AM
Attachments: May Calendar.pdf

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

Today's Sponsor Education Series presentation is hosted CODY Systems. Session information and a registration link are below. Also attached is the May Sponsor Education Series calendar.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data fusion technology fuels fusion centers with a one-stop search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider.

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Thank you for participating in the NFCA Sponsor Education Series.

From:	Cara-Lin Graham
To:	Justin Dutra; dmartin@tivertonpoliceri.com; jpepjonovich@quincyma.gov; Clement, Michael (POL); Paul Gauvin; walter_correia@warehampolice.com
Subject:	RE: ALPR Access
Date:	Friday, October 29, 2021 3:11:13 PM
Attachments:	image001.png Flock-Cranston-MOU-NESPIN-signed.pdf

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

Lt. Dutra,

Please see attached signed MOU from NESPIN. Thank you for allowing access.

Cara Graham, C.I.C.A.
Manager, Criminal Intelligence Services
New England State Police Information Network
124 Grove Street, Suite 105
Franklin, MA 02038
(508) 528-8200 x207
cgraham@nespin.riss.net

Any attached document(s) may be encrypted and requires a password which will be provided in a subsequent e-mail.

If NESPIN has helped you in a recent case please let us know. Your successes are our successes!

Disclaimer: Data in public records, commercially available data sources and the internet can contain errors and are generally not totally free from defect. Data from these sources should not be considered definitively accurate, and all data we provide to you should be independently verified before taking any action based on the results.

This e-mail and any files transmitted with it are the property of NESPIN, are confidential, and are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s), or otherwise have reason to believe that you have received this message in error, please notify the sender at 508-528-8200 and delete this message immediately from your computer. Any other use, retention, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited.

From: Justin Dutra <jdutra@cranstonpoliceri.com>

Sent: Friday, October 29, 2021 11:12 AM
To: dmartin@tivertonpoliceri.com; jpepjonovich@quincyma.gov; Cara-Lin Graham <cgraham@nespin.riss.net>; michael.clement@state.ma.us; pgauvin@frpd.org; walter_correia@warehampolice.com
Subject: ALPR Access

Good Morning,

In response to recent requests for access to Cranston Police ALPR network, I have prepared a MOU which has been attached to this email. Please read, sign, and return for immediate access.

Thank you.

Respectfully,

Lieutenant Justin T. Dutra
Special Projects Lieutenant
Cranston Police Department
Desk (401) 477-5035
Cell (401) [redacted]
Email: jdutra@cranstonpoliceri.com

From: Myslinski, Tara (DOT)
To: Osborne, Chester (DOT)
Cc: Fitzgerald, Thomas (POL); Fenton, Eileen (DOT)
Subject: RE: c. 90 updates for FAST
Date: Monday, March 1, 2021 3:50:28 PM
Attachments: 700 CMR 7 Redline.docx

Here are the redlined regulations. I did not add anything about the natural gas weight exception because I think it's sufficiently covered in the proposed statute, but I can if you prefer.

Please send us any/all thoughts on these regs and the legislative drafts and we will do everything we can to move them along.

Thank you!

Tara Myslinski
Senior Lead Counsel, Regulatory & Compliance
MassDOT
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
Mobile: 857-360-6810
Tara.myslinski@dot.state.ma.us

MassDOT and the MBTA are subject to MGL: Chpt.66, Sec.10 Public Records Law. Email sent or received by MassDOT and MBTA employees are subject to these laws. Unless otherwise exempted from the public records law, senders and receivers of MassDOT and MBTA email should presume that the email are subject to release upon request, and to state record retention requirements.

Confidentiality Notice | This communication (including any attachments) is only intended for the user of the individual, or entity, to which it is directed. It may contain information that is privileged, confidential and exempt from disclosure under applicable law, and should not be read, copied or otherwise used by any other person. If received in error: please notify the sender immediately and delete the e-mail, and any attachment(s), from your system, without copying, forwarding, disclosing or using it in any other way.

From: Myslinski, Tara (DOT)
Sent: Monday, March 1, 2021 2:05 PM
To: Osborne, Chester (DOT) <Chester.Osborne@dot.state.ma.us>
Cc: Fitzgerald, Thomas (POL) <thomas.fitzgerald@pol.state.ma.us>; Fenton, Eileen (DOT) <Eileen.Fenton@dot.state.ma.us>
Subject: c. 90 updates for FAST

Chester and Lieutenant:

Please see the attached suggested changes in c. 90 to conform to the FAST act. I hope this captures everything. From here, I'm going to go through our regs and make additional redlines – hoping to send you those today too.

Note that statutory amendments are difficult to accomplish and I can't predict their passage; regs are far easier. Because this is necessary to comply with federal requirements, however, perhaps we can fast track the legislation.

I am hoping you might be able to go through these in concept with FHWA tomorrow.

Tara

Tara Myslinski
Senior Lead Counsel, Regulatory & Compliance
MassDOT
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
Mobile: 857-360-6810
Tara.myslinski@dot.state.ma.us



MassDOT and the MBTA are subject to MGL: Chpt.66, Sec.10 Public Records Law. Email sent or received by MassDOT and MBTA employees are subject to these laws. Unless otherwise exempted from the public records law, senders and receivers of MassDOT and MBTA email should presume that the email are subject to release upon request, and to state record retention requirements.

Confidentiality Notice | This communication (including any attachments) is only intended for the user of the individual, or entity, to which it is directed. It may contain information that is privileged, confidential and exempt from disclosure under applicable law, and should not be read, copied or otherwise used by any other person. If received in error: please notify the sender immediately and delete the e-mail, and any attachment(s), from your system, without copying, forwarding, disclosing or using it in any other way.

From: Bender, Sean (POL)
To: Range, Scott (POL)
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Monday, April 5, 2021 12:00:03 PM
Attachments: HIDTA_NCRIC CONOP MAY2020.docx
Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020
https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with

permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information

transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information

maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: John Tedona
To: Pack, Noah (POL)
Subject: RE: Fixed & Mobile Locations
Date: Friday, December 10, 2021 11:53:39 AM
Attachments: image002.png
image003.png
image004.png
image007.png
image008.png
image009.png
Neology PAGIS-2.14 Software Training.pptx

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

The Audio file I sent you is the latest and only training material we have for BOSS. An update version will be available soon with additional function/feature descriptions and pop ups. Our BOSS Trainer can set up a webinar as needed for remote real-time training.

Regards,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Friday, December 10, 2021 11:19 AM
To: John Tedona <jtedona@neology.net>
Subject: Re: Fixed & Mobile Locations

Got it. Thanks John.

Do you have any other Boss 4 training materials that we can use - a PDF presentation or slide deck, for example? We need to plan how we are going to train our users and I imagine you have something we can use other than the video.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander

470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Thursday, December 9, 2021 12:28 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Fixed & Mobile Locations

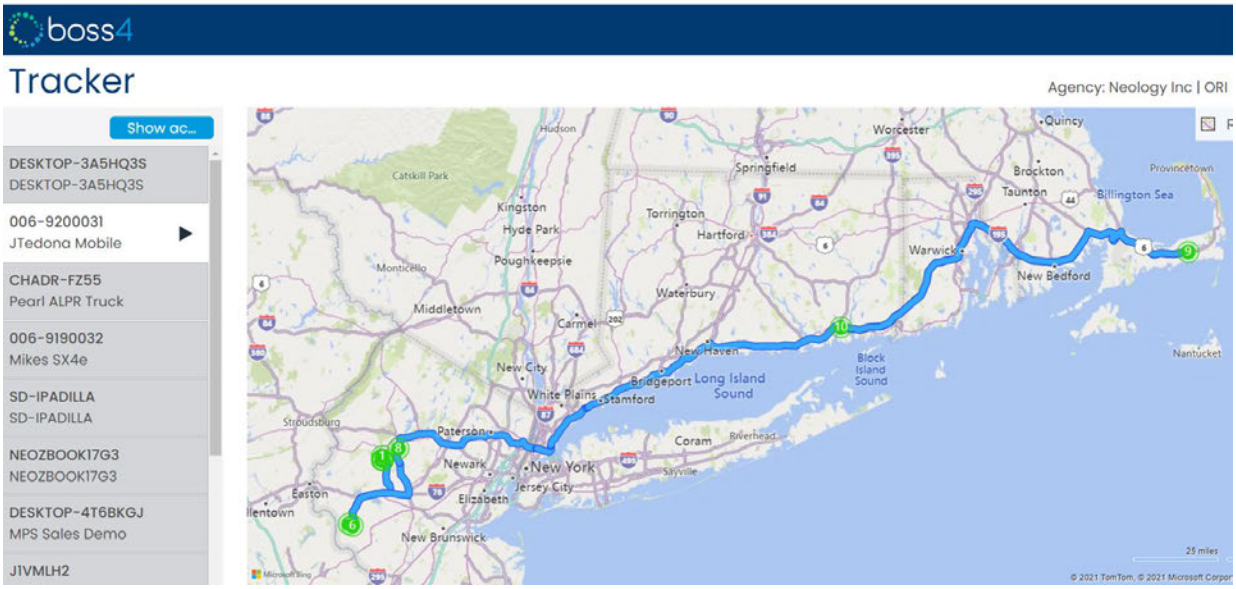
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Noah,

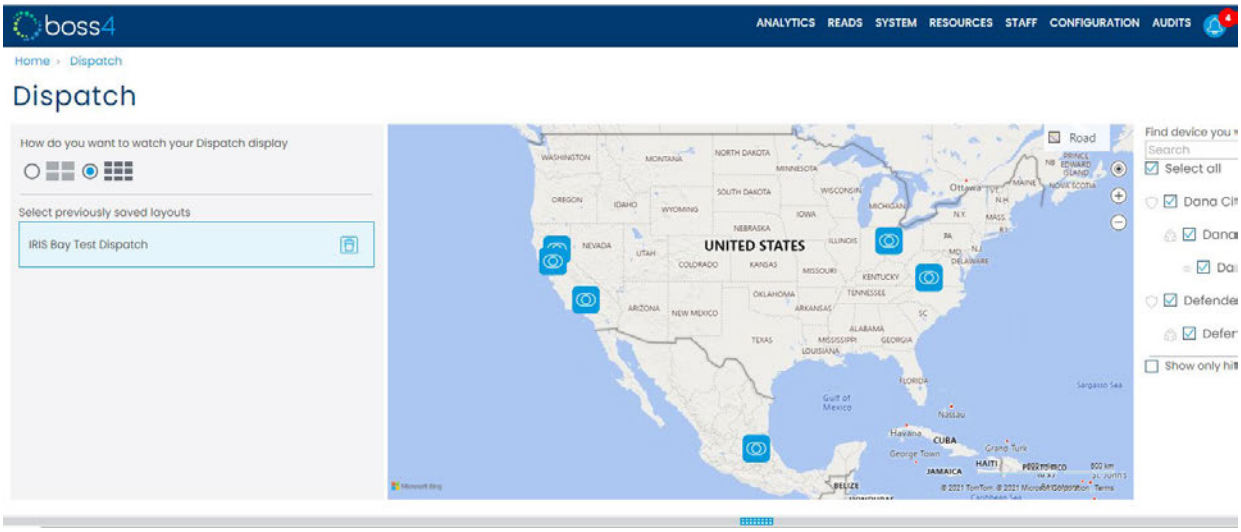
Circling back on your location question in BOSS. I listed a few BOSS screen shots that shows location information. View1 shows "Tracker" this can be turned on to show mobile locations in real-time or travel history, although I don't know of any agencies use this feature. This one shows my ALPR vehicle in some past travel.

View2 shows locations of Neology fixed demo cameras that are installed in the US. View3 shows a zoomed in view of one of the cameras in View2.

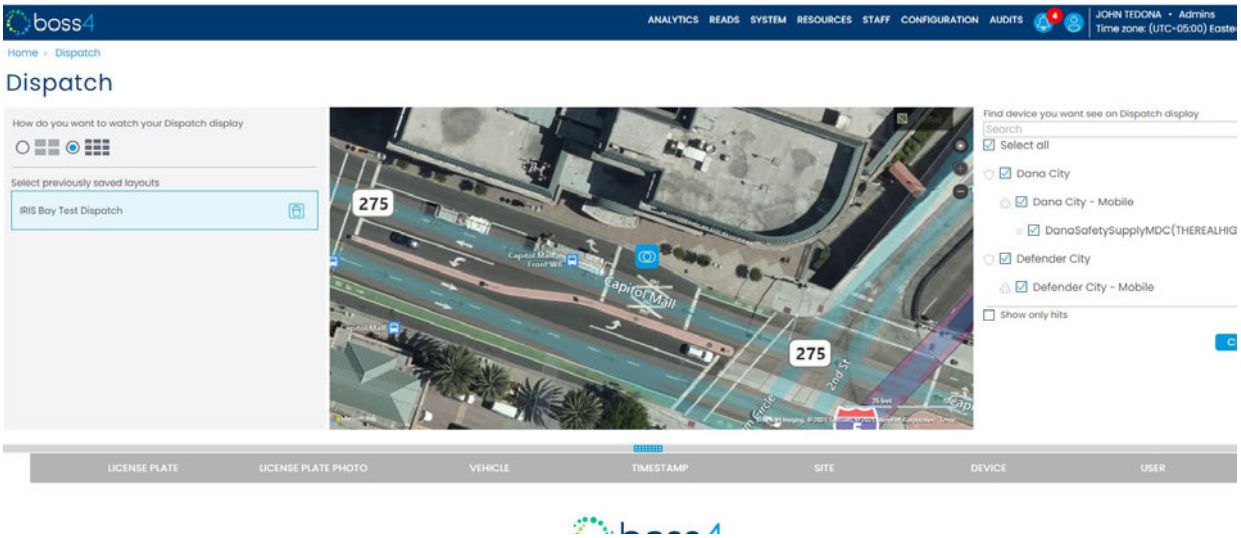
VIEW 1



VIEW 2



VIEW 3



John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

To: Wilcox, Christopher (POL)
Subject: RE: Genetic training
Date: Thursday, August 19, 2021 9:50:22 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

That sounds good, I recommend that TRF-11 be updated to reflect. Currently Field services owns it. I'll setup a meeting to begin a debrief.

-----Original Message-----
From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us>
Sent: Thursday, August 19, 2021 9:27 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Genetic training

Mark Cyr will oversee LPR Along with watch and fusion

LTC Chris Wilcox
Division of Homeland Security and Preparedness

> On Aug 19, 2021, at 9:21 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us> wrote:
>
> Yes
>
>> On Aug 19, 2021, at 9:12 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us> wrote:
>>
>> So is he coming up from Pennsylvania?
>>
>> LTC Chris Wilcox
>> Division of Homeland Security and Preparedness
>>
>>
>>>> On Aug 19, 2021, at 9:02 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>
>>> Just so you are aware this is a vistaCOM employee that would be onsite. BCM is the prime and passing through the cost.
>>>
>>>>> On Aug 19, 2021, at 7:56 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us> wrote:
>>>>
>>>> I forwarded this to Michelle we can talk about it next week
>>>>
>>>> LTC Chris Wilcox
>>>> Division of Homeland Security and Preparedness
>>>>
>>>>
>>>>>> On Aug 19, 2021, at 7:46 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>>>
>>>>> Do we want to adjust the time for the BCM tech?
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Tuesday, August 17, 2021 11:29 AM
>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>

>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Sounds good. Working on that stuff for you.
>>>>>
>>>>> For the AV technician on-site support we are looking at $4500. Are you good with that? If so I will send over a quote.
>>>>> It's not cheap, however it is a 4AM start on a holiday.
>>>>>
>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto
>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>
>>>>> On 8/17/21, 11:20 AM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> I'm looking for this
>>>>>
>>>>> SC-OTC-001 - Security Center - Omnicast Technical Certification
>>>>>
>>>>> And Maybe this
>>>>>
>>>>> SC-OTC-002 - Security Center - Omnicast Advanced Configuration and Troubleshooting
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Thursday, August 12, 2021 1:39 PM
>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>
>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Let me find out for you. What level of training are you interested in?
>>>>>
>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto

>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>> On 8/12/21, 1:35 PM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> What Genetec certificate courses do you guys provide or resell?
>>>>>
>>>>> Thanks
>>>>>
>>>>>
>>>>>

From: Egnitz, Brian (POL)
To: Wilcox, Christopher (POL)
Subject: RE: Genetic training
Date: Thursday, August 19, 2021 9:50:41 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

That sounds good, I recommend that TRF-11 be updated to reflect. Currently Field services owns it. I'll setup a meeting to begin a debrief.

Thanks, Brian

-----Original Message-----
From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us>
Sent: Thursday, August 19, 2021 9:27 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Genetic training

Mark Cyr will oversee LPR Along with watch and fusion

LTC Chris Wilcox
Division of Homeland Security and Preparedness

> On Aug 19, 2021, at 9:21 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us> wrote:
>
> Yes
>
>> On Aug 19, 2021, at 9:12 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us> wrote:
>>
>> So is he coming up from Pennsylvania?
>>
>> LTC Chris Wilcox
>> Division of Homeland Security and Preparedness
>>
>>
>>>> On Aug 19, 2021, at 9:02 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>
>>> Just so you are aware this is a vistaCOM employee that would be onsite. BCM is the prime and passing through the cost.
>>>
>>>>> On Aug 19, 2021, at 7:56 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us> wrote:
>>>>
>>>> I forwarded this to Michelle we can talk about it next week
>>>>
>>>> LTC Chris Wilcox
>>>> Division of Homeland Security and Preparedness
>>>>
>>>>
>>>>>>> On Aug 19, 2021, at 7:46 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>>>
>>>>> Do we want to adjust the time for the BCM tech?
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Tuesday, August 17, 2021 11:29 AM

>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>
>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Sounds good. Working on that stuff for you.
>>>>>
>>>>> For the AV technician on-site support we are looking at $4500. Are you good with that? If so I will send over a quote.
>>>>> It's not cheap, however it is a 4AM start on a holiday.
>>>>>
>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto
>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>
>>>>> On 8/17/21, 11:20 AM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> I'm looking for this
>>>>>
>>>>> SC-OTC-001 - Security Center - Omnicast Technical Certification
>>>>>
>>>>> And Maybe this
>>>>>
>>>>> SC-OTC-002 - Security Center - Omnicast Advanced Configuration and Troubleshooting
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Thursday, August 12, 2021 1:39 PM
>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>
>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Let me find out for you. What level of training are you interested in?
>>>>>

>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto
>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>> On 8/12/21, 1:35 PM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> What Genetec certificate courses do you guys provide or resell?
>>>>>
>>>>> Thanks
>>>>>
>>>>>
>>>>>

From: Whittemore, Scott
To: Brooks, Brian (POL)
Subject: RE: policy draft
Date: Tuesday, April 6, 2021 2:32:47 PM
Attachments: LPR Policy.docx

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

Good Afternoon Sir-

I miss getting your requests for info on Holidays---

See attached. Let me know what else you need. This was based on the 'model' policy from DCJIS that was put out a few years ago.

Scott

From: Brooks, Brian (POL) <brian.brooks@state.ma.us>
Sent: Tuesday, April 6, 2021 2:12 PM
To: Whittemore, Scott <swhittemore@wellesleyma.gov>
Subject: policy draft

[**EXTERNAL EMAIL :** This message originated outside of the TOWN OF WELLESLEY mail system. **DO NOT CLICK** on **links** or open **attachments** unless you are sure the content is safe.]

Deputy, do you have a policy in Wellesley for Vigilant? I believe Major Range was going to reach out to you, but I figured I'd try to get a head of it whereas we will require one here. Brian

From: Katabazi, Lydia (FMCSA)

To: AK - Debbie Leonardo; Inga Johnson; Katherine Hensley; AK - Katie Smith; AL - David Baxley; AL - Jay Starling; AL - Sherry Helms; AL - Trishawn Bell; AR - Christy Earnhart; AZ - Diane Quintana; AZ - Gloria Paul; AZ - Steven Kalina; CA - Angela Marbray; CA - Coral Barber; CA - Marvin Hardley; CA - Suk Medeiros; CO - Abigail Lopez; CO - Dina Smith; CO - Jennifer Ketterman; CO - Jenny Adler; CO - Kirstie Nixon; CO - Michael Wolfinger; CO - Pamela Krupe; CO - Shanielle Rodriguez; CT - Iliana Rodriguez; CT - Kelly O"Connell; CT - Lori Druan; CT - Vanita Smith; DC - Darnell Fountain; elaine.speller dc.gov; DC - Michael Williams; DE - Mark Eastburn; DE - Robyn Bose; FL - Jay Levenstein; FL - Judy Cruce; FL - Robyn Wilson; GA - Brent Bennett; GA - Jared Hill; george.white ct.gov; IA - Alexander Jansen; IA - Angel Robinson; IA - Brenda Freshour-Johnston; IA - Debbie Leib; IA - Deborah Roeder; IA - Mary Guillaume; ID - Alberto Gonzalez; ID - Craig Roberts; ID - Jerri Hunter; ID - Reymundo Rodriguez; IL - Jason Copelin; IL - Michelle Blackley; IL - Scott Tucker; IN - Sandy Bowling; IN - Trish Smith; IRP Inc. - Robin Murphy; tadams irpinc.org; jeffrey.a.oberdank dos.nh.gov; jsteeger@mt.gov <MT State Partner>; KS - Deann Williams; KS - Dena McDaniel; KS - Donald Lee; KS - Rodney Allen; KY - Drew Clark; KY - Jennifer Walton ; KY - Lee Wigginton; KY - Mary Cook; KY - Robin Snook; KY - Stacey Schultz; KY - Tom McDaniel; LA - Andrea Chapman; LA - Brady Pupera; LA - Jeffrey Simmons; Lee.Nagano@hawaii.gov <HI DOT>; Rizzuto, Elizabeth (DOT); Sheehan, Erin (DOT); Daley, Gretchen (DOT); Rogers, Jessica (DOT); MA - Lawrence Lowery; Armstrong, Leslie (DOT); Parrott, Lynn (DOT); Duff, Melissa (DOT); Leblanc, Michelle (DOT); Cox, Stephanie M. (DOT); MD - Jan Hejl; MD - Kevin Gamble; MD - Latonya Montgomery; ME - April Goodwin; ME - Chelsea Chase; ME - Stephen Ashcroft; MI - Amy Havens; MI - Christopher Blundell; MI - Dawn VanAken; MI - Kimberly Hengesbach; MI - Michael Butcher; MI - Rayne Sherman; MN - Emma Corrie; MN - Erica Baraglia; MN - Natalie Wendell; MO - Aaron Hubbard; MO - Kelly Ray; MO - Michael Yoder; MO - Nathan Fontaine; MS - Danielle Hughes; MT - Eric Belford; MT - Jodee Alm; MT - Tom Winfield; NC - Cheryl Stanfield; NC - Dennis T. Smith; NC - J Council; NC - L Tinsley; NC - P Jacobs; NC - Portia Manley; ND - Dave Wolf; ND - Kyle Larson; NE - Beth Hartley; NE - Cathy Beedle; NH - Cindy Douglas; Marshall, Eric; NH - Scott Bryer; NJ - Christine Inglin; NJ - James Walker; NJ - Tykarra Barnwell; NM - Bernadette Gonzales; NM - Teresa Valdez; NV - Andrea Burnell; NV - John Neese; NV - Regina Ward; NV - Richard Wagner; NY - Andrew Deseve; NY - Bryan Solek; NY - Karen Jewett; NY - Karen Paradise; NY - Mary Withkowski; OH - Carolyn Evanston; OH - Devon Riggins; OK - Laura Osborne; OK - Nick Hensler; OK - Scott Greenawalt; OR - Angela Forrette; OR - Audrey Lawson; OR - Hannah Wilson; OR - Jonathan Reimer; OR - Laurie Hall; PA - Craig Johnson; PA - Michelle FIsher; PA - Nicholas Melnick; PA - Sombrata Bandyopadhyay; PA - Tammy Kohr; PA - Tanya Cooper; RI - Larissa Skeritte; lisa.fresolone dmv.ri.gov; SC - Amber Keane; SC - Cassidy Cade; SC - Deborah Smith; SC - Ernestine Aiken; SC - Mechelle Samuel; Larrimore, Nancy; SC - Wilma Allen; scott.haneberg hawaii.gov; SD - Chris Keil; SD - Darrin Gerry; SD - Dawn Sass; SD - Monica Weischedel; Susan.chang hawaii.gov; TN - Allison Raymer; TN - Amanda Kessler; TN - Beverly Bowman; TN - Dana Lee; TN - Danielle Baines; TN - Jennifer Lanfair; TN - Joetta Alderson; TN - Loretta Wheeler; TN - Mark Thomas; TN - Rachel Greer; TN - Romany Hanna; TN - Ryan Biggs; TN - Sisilia Liu; TN - Travis Plotzer; TN - Tymicia Willis; TX - Grady Meyer; TX - John Poole; TX - Tammy Russ; UT - John Moody; UT - Paula Vanikiotis; UT - Stephen Goodrich; VA - Florence Jett; VA - Pat Wimberly; VA - Patrick Harrison; VA - Shannon Hardy; VA - Yolanda Fleming; VT - Lori Stiles; VT - Mark Huntington; VT - Michael Smith; WA - Cathy Field; WA - Debbie Sanders; WA - George Price; WA - Kyle Strozyk; WA - LaVonne Fromm; WA - Sean McCoy; WA - Vanessa Simpson; WA - Wesley Marks; WI - Dustin Sweeney; WI - Ehren Bittorf; WI - Kathleen Hamilton; WI - Megan Powers; WI (JJKeller) - Kelly Gehrke; WV - Teresa Schott; WV - Zoe Bender; WY - Deborah Lopez; WY - Katherine Darrah; WY - Shannon DeGrazio; Jeremy Arnold; AZ - Jerry Haupt; CA - Denis Tam; Camsys - Brian Stewart; CAPS - Jeremy Pate; Celtic - Jeff Morgan; Celtic - Joe McCormick; Celtic - Kris Weaver; Celtic - Lynn Watson; Celtic - Manish Gohil; Celtic - Samir Nayak; bob.sardo ct.gov; DE - Geri Smith; DE - Kevin Needham; Punita.Choxi state.de.us; DriveWyze - Sara Steele; Explore - Jeff Pieschke; Explore - Nikki Benz; Explore - Scott Baker; Explore - Seth Ostrander; Explore - Tom Reynolds; FAST - Email; FAST - Julie Doney; FAST - Julie Doney; FAST - Mohamed Metwally; FL - Elvaro Jimenez; FL - Rufus Mayo; FL - Scott Tomaszewski; GA - Hugo Hall; GA - Rao Gorti; GA - Tracie Scott; ID - Neil Snyder; IIS - Brian Heath; IIS - Fred Ko; IIS - Werner Fraga; IL - Angie Williams; IL - Marinda Beccue; IL - Michael Stout; IL - Peter Neff; IL - Rod Smith; IN - Ranganath Kore; IN - Ravi Surapaneni; IN - Rongqiu Shen; IN - Uma Muttavarapu; IRD - Debbia Sarvas; IRD - Josh Zacharias; ISP - Tracs Support; Iteris - Aaron Jenkins; Iteris - CVO Support; Iteris - Delaine Adkins; Iteris - Inspections; Iteris - Jason Bowden; Iteris - Thad Hoffman; KY - Andrew Williams; KY - Donald Price; LA - Terri Ungerman; Legatus - Joanna Masny; Legatus - Mike Holloman; Legatus - William Curry; Kovac, James (DOT); Hanson, Michelle (ATLAS); MA - Sye Chanthaboun; MD - Madison Lumpkin; MD - Natalie Grasso; MD - Patrick Strauch; ME - Ann Lamore; MI - Dan Meengs; MI (Fast) - Luke Kledzik; MI (Fast) - Nathan Schmidt; MI (Fast) - Tom Yao; MN - Alex Gohar; MN - Jenny Cai; MN - Mike Baker; MN - Steve Mueller; MO - Doug Abbott; MS - Billy Saxton; MS - Hubert Crook; MS - Richard Smith; MS - Wyatt Sanford; NC - Bruce Boaz; NC - Mike Spears; ND - Scott Moran; NDSU - Brenda Lantz; NE - John Casteel; NLETS - Dustin Green; NLETS - Kate Silhol; NLETS - Kyle Darnell; Helpdesk Nlets; NM - Ojito Prevatt; NY - Ben Johnston; NY - Darcel Forde; NY - Joanne Catallo; NY - Lisa Clark; NY - Sri Nadella; OH - Alan Martin; OH - Candace Marzec; OH - Kate Hatfield; OH - RK Bogue; OH - Russ Dunn; OH (Leonardo) - Cisco Gonzalez; OH (Leonardo) - Matt Maxwell; OR - Chris Howell; OR - Michael Hartman; PA - Greg Gelnett; PA - Pam Molison; PrePass - Jan Skouby; SC - Darl Neiswonger; SC - IT Support; SecureWatch24 - Pat Fox; Seikosoft - Jordan Hayashi; SWRI - Darin Parish; SWRI - Tammy Duncan; TX-DPS - Richard Jackson; UT - Doug Stuart; VT - Chris Pitt; VT - Kelly Reagan; WA - Someshwar Busi-kumar; WI - CVIEW Support; WI - DMV Production Support; WI - MCR Unit; WY - AJ Myers; AL - Brent Mcelvaine; AL - Captain Jessie Peoples; AL - Lt. David Colston; AL - Mark Neilson; AL - Sgt. Michael Griffies; AR - Major Jay Thompson; Dan Williams; CA - Capt. Sean Duryee; CA - Lt. Nicholas Doko; CA - Sgt. Jaime Nunez; CO - Jeff Sewell; CO - Maj. Jon Barba; CO - Trish Aragon; CT - Corporal Greg Zeoli; CT - Lt. Christopher Smith; Donald Bridge; James Schaefer; Daniel.Parks state.de.us; FL - Keith Westphal; GA - Lt. Brent Moore; GA - Major Johnny Jones; scott.haneberg hawaii.gov; Susan.chang hawaii.gov; IA - Chief David Lorenzen; ID - Capt. Shawn Staley; IN - Donna Luley; IN - Kim Judge; IN - Major Jon Smithers; KS - Capt. Wes Ludolph; KS - Tom Catania; KY - Jennifer Walton; John Smoot; KY - Truesdell Tristan; LA - Capt. David Templeton; LA - Lt. Rueben.Auter; LA - Sgt. Kirk Thibodeaux; Fitzgerald, Thomas (POL); Jrotz sha.state.md.us; MD - Kevin Hickey; MD - Lt. John Griffin; James Wright; MI - Captain Michael Krumm; MI - Jack Johnson; MI - Lt. Charles Black; MN - Capt. Jonathan Olsen; MN - Lt. Arthur "Lee" Gear; matt.sokol state.mn.us; Kevin Kelley; MS - Chief Willie Huff; Greg Watson; MS - Major Roderick

	Goode; Ted Grimes; jsteeger@mt.gov <MT State Partner>; Karen.Ward ncdps.gov; NC - Kendell Jackson; NC - Lt. Terry Robinson; NC - Myra Beckers; NC - Sgt. Steve Kirby; NC - Tim Peterson; ND - Lt. Mike Roark; NE - Capt. Gerry Krolikowski; Daniel Doggett; NH - Sgt. William Burke; NJ - Sgt. Scott Dorrler; NM - Jessica Gibson; NM - Joseph Romero; NM - Todd Cullers; NV - Linda Allred; NV - Lt. Don Plowman; NY - Chris Scharl; NY - Jean-Paul Paraskevas; NY - Jill LaManna; NY - Jonathan NiCastro; NY - Justin Zimmerman; NY - Lt. Joseph Huber; NY - Marc Berger; NY - Suzanne Keiffer; OH - Bob Hartman; Brandon.Evans dps.ohio.gov; OH - Lt. A Reimer; Justin Gandy; PA - Brian M. Carpenter; PA - Chris Keffer; Doug Kemp; PA - Lt. Robert Krol; PA - Lt. Stephen Adamczyk; PA - Sgt. Michael Pavelko; RI - Corp. Mark Perotti; RI - Sgt. John Furtado; RI - Trp. John Gadrow; SC - Capt. John Price; SC - Colonel Leroy Taylor; SC - Major Dean Dill; SC - William David Findlay; john.broers state.sd.us; SD - Joel Peterson; TN - Capt. Brandon Douglas; TN - Lt. Allen England; troythompson flhsmv.gov; steven.rundell dps.texas.gov; TX - Major Chris Nordloh; csheppick utah.gov; ron.maxey vsp.virginia.gov; VA - First Sgt. Shawn Gobble; VA - Sgt. Robert Alessi; VT - Corporal Matt Nesto; WA - Capt. Trisena Sharff; WA - Donald Knoop; WI - Lt. Karl Mittelstadt; WV - Jessica Gordon; rbunner psc.state.wv.us; rblankenship psc.state.wv.us; WY - Christina Helsel; Dan Wyrick
Cc:	DeLorenzo, Joseph (FMCSA); Keane, Tom (FMCSA); Mahorney, Bill (FMCSA); Liberatore, Thomas (FMCSA); Kelly, Thomas (FMCSA); White, Camille (FMCSA); Byrne, Angie (Volpe); PRISMTechnicalSupport; Tepp, Jacob (FMCSA); Price, Bryan (FMCSA); FMCSA_MCFSPM; MCDA
Subject:	Re: PRISM Technical Announcement - ISS Target File
Date:	Monday, February 22, 2021 6:32:37 PM
Attachments:	PRISM Technical Announcement ISS Target File.pdf

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

Greetings PRISM Partners,

A supplemental PRISM Target File called the Inspection Selection System (ISS) Target File is currently available for State Law Enforcement to download and use to support roadside enforcement.

The ISS Target file is intended to provide additional information to State law enforcement to strategically and efficiently identify commercial motor vehicles for inspection by linking the motor carrier's ISS score to the vehicle registration record using the U.S. Department of Transportation (USDOT) number.

State Law Enforcement can utilize the ISS Target File with an Automated License Plate Reader (ALPR) to search and associate the ISS Score with the license plate at roadside to distinguish commercial motor vehicles that are linked to motor carriers with a higher safety risk.

The ISS Target File is used for Roadside enforcement only and is not a requirement to participate in PRISM.

Please see attached Announcement for details and let us know if you have any questions.

Thank you,

Lydia Katabazi

Lydia T. Katabazi
PRISM Program Manager
USDOT | FMCSA | Enforcement Division

1200 New Jersey Ave, SE, W63-455, Washington, DC 20590
☎Office: 202.366.0991 | ✉Email: Lydia.Katabazi@dot.gov

From: Peter Crary
To: Merrill, William R. (EOTSS)
Cc: Zhong, Henry; Chandler, Rob; Mitchell, Timothy P. (EOTSS); Velez, Mario; Dewey, Heather; Egnitz, Brian (POL); Osman, Ashraf; Novak, Marsel; Tom Cobb; Sullivan, Margaret (POL); Ramsay, Christopher B. (EOTSS); Stockwell, Matthew R. (EOTSS)
Subject: Re: Snowball - Neology+ Mass St Police
Date: Friday, September 17, 2021 4:30:24 PM
Attachments: image001.png

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

I sent it to Tim and Brian.

Peter Crary
Global R&D Director, ALPR
Neology, Inc
(Sent from my iPhone)

> On Sep 17, 2021, at 15:29, Merrill, William R (MASSIT) <william.r.merrill@state.ma.us> wrote:
>
> So on Step 4 I believe the confusion lies. Where does the unlock code come from and what is manifest? Is that the command to use in the command line interface?
>
> -bill
>
> **From:** Zhong, Henry <henzhong@amazon.com>
> **Sent:** Friday, September 17, 2021 4:25 PM
> **To:** Merrill, William R. (EOTSS) <William.R.Merrill@mass.gov>; Chandler, Rob <rbchand@amazon.com>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>; Velez, Mario <marvlez@amazon.com>; Dewey, Heather <hdewey@amazon.com>
> **Cc:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>; Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Ramsay, Christopher B. (EOTSS) <Christopher.B.Ramsay@mass.gov>; Stockwell, Matthew R. (EOTSS) <Matthew.R.Stockwell@mass.gov>
> **Subject:** Re: Snowball - Neology+ Mass St Police
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Bill

You are correct, the Snowball device and server with the snowball client will not need internet access. At high level you have the steps, I added step#4 authenticate the client to the snowball and #6 test run step .

1. Connect to switch via 10g copper
2. Configure static IP (no DHCP)
3. Install client on server
4. **Use manifest and unlock code to authenticate the Snowball client's access to a Snowball**
5. Initiate copy via command line
6. **Test run**
7. Profit

Henry Zhong | Solutions Architect, SLG Northeast
henzhong@amazon.com | Cell: [redacted]

From: "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>
Date: Friday, September 17, 2021 at 4:10 PM
To: "Zhong, Henry" <henzhong@amazon.com>, "Chandler, Rob" <rbchand@amazon.com>, "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>, "Velez, Mario" <marvlez@amazon.com>, "Dewey, Heather" <hdewey@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: RE: [EXTERNAL] Snowball - Neology+ Mass St Police

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

Hi Henry,

So to make it clear:

We already have the Snow device so the steps follow:

Connect to switch via 10g copper

Configure static IP (no DHCP)
Install client on server
Initiate copy via command line
??
??
Profit

At no point do we need to get the Snow device connected to the internet? Nor does the server with the client need to be connected to the internet? Sorry for all of the questions. We were looking to do a call but if my steps above are correct, we should be good to go.

-bill

From: Zhong, Henry <henzhong@amazon.com>
Sent: Friday, September 17, 2021 4:03 PM
To: Chandler, Rob <rbchand@amazon.com>; Merrill, William R. (EOTSS) <William.R.Merrill@mass.gov>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>; Velez, Mario <marvlez@amazon.com>; Dewey, Heather <hdewey@amazon.com>
Cc: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>; Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Ramsay, Christopher B. (EOTSS) <Christopher.B.Ramsay@mass.gov>; Stockwell, Matthew R. (EOTSS) <Matthew.R.Stockwell@mass.gov>
Subject: Re: Snowball - Neology+ Mass St Police

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

Hi Bill

The snowball client on the server and snowball device communication is encrypted in-transit; and during the request of snowball device in AWS console, an KMS(encryption key is added to encrypt data at rest.

Snowball device is configure to use DHCP and it will get an IP from your network DHCP server or you can change to static IP on the LCD display.

The server with data is on VM should not a problem; the team can run test to verify the

speed by copying files to another server.

Henry Zhong | Solutions Architect, SLG Northeast
henzhong@amazon.com | Cell: [redacted]

From: "Chandler, Rob" <rbchand@amazon.com>
Date: Friday, September 17, 2021 at 3:44 PM
To: "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>, "Zhong, Henry" <henzhong@amazon.com>, "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>, "Velez, Mario" <marvlez@amazon.com>, "Dewey, Heather" <hdewey@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: Re: [EXTERNAL] Snowball - Neology+ Mass St Police

I'm adding Heather and Mario from our Snow team to assist on these additional questions.

From: "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>
Date: Friday, September 17, 2021 at 12:42 PM
To: "Zhong, Henry" <henzhong@amazon.com>, "Chandler, Rob" <rbchand@amazon.com>, "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: RE: [EXTERNAL] Snowball - Neology+ Mass St Police

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

Thanks for the response Henry. One of the questions we had that were not completely clear in the documentation we reviewed was due to the encryption. Does the Snowball device need to be "enabled" before using via some hash? If we are going to plug it into a 10g copper switch, what other steps will we need to do? Assign it an IP? The server we are pulling the data from is a VM. Does that limit us somehow?

We will get the client/agent on the server in question and then start the copy process and that is that? When does the encryption of the data take place? During the transfer? At rest?

-bill

From: Zhong, Henry <henzhong@amazon.com>
Sent: Friday, September 17, 2021 3:24 PM
To: Chandler, Rob <rbchand@amazon.com>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>
Cc: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>; Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Ramsay, Christopher B. (EOTSS) <Christopher.B.Ramsay@mass.gov>; Merrill, William R. (EOTSS) <William.R.Merrill@mass.gov>; Stockwell, Matthew R. (EOTSS) <Matthew.R.Stockwell@mass.gov>
Subject: Re: Snowball - Neology+ Mass St Police

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

Hi Tim,

To copy 27TB of data to the snowball device will take some time depends on your local network speed between the server/snowball client and the snowball device. I include information outlines on how the network's transfer rate impacts how long it take to copy data to the device.
https://docs.aws.amazon.com/snowball/latest/ug/performance.html

To give some context here - if you are getting (~1 gig network) 100mb/second file copying speed from server to the snowball device on your network; then it will take about 3.12days to complete the 27TB of data. you can attempt multiple Snowball client workstations to improve performance/reduce time as suggested in the link above.

Snowball client workstation does not require internet access but you will need internet access to download the Snowball client from another workstation.
You can download the Snowball client from AWS Snowball resources.

Let us know if you have other question and happy to join a call with the team to walk thru the snowball client installations.

Thanks
Henry Zhong | Solutions Architect, SLG Northeast
henzhong@amazon.com | Cell: [redacted]

From: "Chandler, Rob" <rbchand@amazon.com>
Date: Friday, September 17, 2021 at 1:32 PM
To: "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>, "Zhong, Henry" <henzhong@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: Re: [EXTERNAL] Snowball - Neology+ Mass St Police

+Henry Zhong

From: "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>
Date: Friday, September 17, 2021 at 10:28 AM
To: "Chandler, Rob" <rbchand@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: RE: [EXTERNAL] Snowball - Neology+ Mass St Police

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

Thank you for reaching out Rob.

I have copied the team from my side on this email. We are expecting to receive the Amazon Snowball device and need to figure out what we have to do to copy data from one 27T database to that device. In doing some preliminary reading about this we thought that the device needs network connectivity to the same subnet as the existing server to do the copying. Is that correct? Does the Snowball client need to be on a machine that has internet access as well as access to the snowball and database server in question? We have no prior experience with this and are looking for steps that we need to take to get this connected to the network/existing server.

Thank you

From: Chandler, Rob <rbchand@amazon.com>
Sent: Friday, September 17, 2021 12:37 PM
To: Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>
Cc: Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>
Subject: Snowball - Neology+ Mass St Police

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

Hi Tim,

I'm Neology's Account Manager here at AWS. Copying Tom and Marsel who support MSP. Ashraf is my technical counterpart.

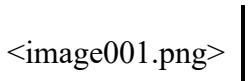
Peter let me know you had some questions regarding setting up Snowball and configuring the transfer.

Can you let us know what specific questions you have and hopefully we can resolve this quickly. If the account team can't resolve, we'll look at pulling in specialists as needed.

In case you haven't seen it, the docs are also quite extensive:
https://docs.aws.amazon.com/snowball/

Thanks,
Rob

_____



Rob Chandler
Account Manager - GovTech
Amazon Web Services
m: 410.212.3506

From: Pack, Noah (POL)
To: Wilcox, Christopher (POL)
Cc: Egnitz, Brian (POL)
Subject: Topics for Legal
Date: Tuesday, December 7, 2021 9:16:02 PM
Attachments: Flock Promo Description.pdf
MSP FLOCK MOU.pdf

Colonel:

The following topics are tentatively on our list to discuss at some point with legal:

1. MOUs:
    a. authorization/signatures for a usage MOU with Flock; MOU is attached
    b. when is an MOU is needed for other platforms?
    c. Flock data is free. Other platforms may be as well. Is there any issue with free LPR data from these companies?

2. LPR Infrastructure protection: discovery/FOIA
    a. For efficient management and deployment we'd like to create a map of LPR locations, but public release of same could result in widespread system damage/vandalism or avoidance
    b. How can we create but protect these documents?

3. Turnpike gantry LPR
    a. legal opinion of process required for investigative access per MGL
    b. developing a unified procedure & POC for exigent access

4. Use of new Boss4 LPR software purchased by Department:
    a. what should be on a splash screen (CJIS policy, anything else, requirement to agree in order to access)
    b. is splash screen sufficient to cover our members?

5. Tenant agencies contributing data:
    a. What do we require from them to accept their data?
        i. agency policy? any minimum standards? MOU?
        ii. we are awaiting some information from other agencies on what they do.
    b. Retention periods for locals policy may be less than 1 year.
        i. software setting appear to allow this, is it an issue to reduce retention period for some agency contributors?

6. Vigilant data:
    a. Department has purchased or obtained access to Vigilant national LPR database

through the Motorola body camera contract.

b. I'm working with DCapt. McCarthy for further info. There may be some questions on this related to commercial data, potential MOUs, etc. as we move forward. Inquiry for legal is incomplete at this point but should be resolved by time of meeting.

7. Flock nationwide study program:
    a. Through a partnership with Axon, Flock is offering a nationwide study/trial deployment that includes the free deployment of 25 cameras for one year, at locations of our choosing.
    b. They will handle deployment and cover the cost of all equipment and services for one year.
    c. They will make their SMEs and government affairs legal team available to us as needed.
    d. There is no obligation, and they will retrieve all devices and remove them after a year if we are not interested in an ongoing business relationship.
    e. This trial/study offer ends at the end of the calendar year, so we will need to make a decision shortly if we are able to do it.
    f. Preliminary info is attached.

8. Policy review and updates are pending in near future but not ready for discussion at this time.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: Sheehan, Erin (DOT)
To: Clements Jr, Robert F (POL)
Subject: AAMVA 2020 License Plate Standard Final (4) (002).pdf
Date: Wednesday, May 26, 2021 2:09:15 PM
Attachments: AAMVA 2020 License Plate Standard_Final (4) (002).pdf

---

2.2 Character Sizing and Placement Characters are at least 2.5 inches in height, proportionally wide, and spaced no less than 0.25 inches apart. Character stroke weight (thickness of lines) is between 0.2 and 0.4 inches. Characters are positioned on the license plate no less than 1.25 inches away from the top and bottom edges of the license plate.

From:	Chris Perez
To:	McCarthy, Steven (POL)
Cc:	Mason, Christopher (POL); Warmington, Scott (POL); Quinn, Dermot (POL); Kevin Coughlin; Small, Michelle (POL); Venkatachalam, Krishna (EPS); Robles, Francis Jr. (POL); Connor, Debora (POL); Ryan Garofano
Subject:	ALPR & 4RE Decision
Date:	Wednesday, March 17, 2021 11:30:43 AM
Attachments:	L5Q Quick Deploy LPR System Data Sheet.pdf Mobile Companion Sheet.pdf L5F Fixed LPR Data Sheet.pdf Mobile LPR Data Sheet.pdf

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

Captain McCarthy,

Your email to the group was forwarded over to me from the WatchGuard staff so I just wanted to take a moment to respond. Thanks for meeting my colleague Ryan Garofano yesterday and evaluating the 4RE LPR solution. As you referenced, the field of view for the 4RE is too broad, and asking it to do both LPR + evidence collection has seemed to be a tough ask.

This was the first iteration of the integration we hope to achieve with our partnership with WatchGuard. We are building out a new version of this in the future and this feedback is extremely valuable.

One thing to clarify is that in your email you stated, "What it does underscore is that the Vigilant system needs a purpose-built camera for robust ALPR." I just wanted to note that we do in fact have a series of robust LPR cameras that we've been selling on the market, many of which have been deployed throughout the state of Massachusetts. With your LPR data subscription you'll be able to see both the commercial data *and* all of our cameras deployed by police departments around the country.

I attached some information on our fixed cameras, our solar/quick deploy option, mobile cameras, and mobile app, all of which are integrated into our system. If you're open to further discussions about expanding, want some flexibility, or would like to demo our robust equipment, we would certainly welcome them. I understand you guys have utilized PIPS in the past, but with our recent updates I'm confident you would see an enhancement in both hardware and software functionality. Keep in mind we can always integrate your existing data to avoid having to use 2 separate backends.

If you ever have any questions, please feel free to reach out to either me or Ryan and we'd be happy to discuss.

Happy St. Patty's Day.

Thanks,

Chris Perez
Eastern US Sales Director
Video Security & Analytics
Vigilant Solutions



m: (516) 859-1520
TEMPORARY NUMBER through 3/18 - (242) 824-8837

Grant Assistance | Training | LinkedIn

Support: (925) 398-2079 | Email Support

For more information on how and why we collect your personal information, please visit our Privacy Policy.

From: Justin Dutra
To: dmartin@tivertonpoliceri.com; jpepjonovich@quincyma.gov; cgraham@nespin.riss.net; Clement, Michael (POL); Paul Gauvin; walter_correia@warehampolice.com
Subject: ALPR Access
Date: Friday, October 29, 2021 11:15:53 AM
Attachments: FLOCK MOU.docx

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

Good Morning,

In response to recent requests for access to Cranston Police ALPR network, I have prepared a MOU which has been attached to this email. Please read, sign, and return for immediate access.

Thank you.

Respectfully,

Lieutenant Justin T. Dutra
Special Projects Lieutenant
Cranston Police Department
Desk (401) 477-5035
Cell (401) [redacted]
Email: jdutra@cranstonpoliceri.com

From: Egnitz, Brian (POL)
To: Wilcox, Christopher (POL)
Subject: ALPR Bills
Date: Thursday, June 24, 2021 9:14:46 AM
Attachments: Re ALPR Proposed Legislation.msg
Fwd ALPR Proposed Legislation.msg

From: John Tedona
To: Pack, Noah (POL)
Subject: ALPR Equipment PDFs
Date: Monday, November 29, 2021 1:44:42 PM
Attachments: image001.png
image002.png
image003.png
P720 Mobile ALPR.pdf
Iris Data sheet US.pdf

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

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Bender, Sean (POL)
To: Thibault, Amy (POL)
Cc: Smith, Eleanor (POL)
Subject: Analysis Toolkit
Date: Wednesday, January 27, 2021 3:46:13 PM
Attachments: Analyst Professional Development Road Map.pdf

Good Afternoon, Amy/Elly -

I don't know that anyone else would find this interesting, but the NFCA Conference block on *Managing Your Intelligence Analysis Services Toward a Successful Result* referred a couple times to the *Analyst Professional Development Roadmap.* I'm sure most have seen or read the document at this point, but it links to the Office of Justice Programs - Analysis Toolkit site https://it.ojp.gov/AT/ which has *a lot* of interesting tools and resources for categories like policy, technology, training, etc. There are some good reads on ALPR/FR policy, Use of Social Media in Intelligence/Investigative Activities, P/CRCL, etc.

> Analysis Toolkit - Office of Justice Programs
>
> Notice of Federal Funding and Federal Disclaimer. This website is funded through a grant from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse this website (including, without limitation, its content, technical infrastructure ...
>
> it.ojp.gov

Respectfully,

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

From: Peter Crary
To: Mitchell, Timothy (EPS); Egnitz, Brian (POL)
Subject: aws snowball
Date: Friday, September 17, 2021 12:29:02 PM
Attachments: image007.png
image008.png
image009.png
snowball-edge-data-migration-guide.pdf

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

Peter Crary
Global R&D Director, ANPR/ALPR

Mobile: + 865 386 3821
Email: pcrary@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

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

From: LPR
To: Brooks, Brian (POL); Hersey, Kevin
Cc: Castaneda, Robert E.(Eric); Hurst, Donald S (Stuart)
Subject: DEASIL LPR MOU Data Share - Follow-up
Date: Monday, September 13, 2021 1:16:37 PM
Attachments: image001.png
image002.png
image004.png
CC APPROVED LPR Standard Data-Sharing MOU Template 2020-07-09.doc
07.02.21 EPIC-DEASIL.pdf

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

Good afternoon Lieutenant Brooks,

I was provided your name by SA Hersey of the New England Office, and I thought to follow up on our request to integrate your local aLPR data (Vendor: UKN) with the National License Plate Reader Program (DEASIL) here at the El Paso Intelligence Center (EPIC). I've attached the pre-approved Chief Council Data Share MOU for your review – but understand if you might have any logistical questions.

As we approach the end of our fiscal year, we are reviewing prior inquires from various agencies and identified your agency as one to follow up on. We are abundantly aware that the past year has been a trying time for all, and understand that this request may have been earmarked for a later date. At your convenience, can you indicate whether you plan to move forward with data share, or whether you'd like to be taken off of our list of interest?

Do know that this is not a one way flow of data, you and your colleagues are able to utilize DEASIL (which is upto about 3,000 site locations across the antion) on your own or through our 24hr Watch Unit, free of charge, once you've been vetted through EPIC. Again, I am available for any questions or concerns you may have. We look forward to hearing from you!

Thank you,

Cari N. Schieno | Program Analyst
DEASIL | National License Plate Reader Program (LPR)
El Paso Intelligence Center (EPIC)
Desk: (571) 387-4220 | Cell: (915) [redacted]
Cari.N.Schieno@dea.gov
"Do right and fear not"

"We'd love to hear any success stories from you, the users. These justify the coverage and growth of this program!"
You can send your stories to LPR@usdoj.gov or to cari.n.schieno@usdoj.gov
DEASIL Password/Account reset LPR@usdoj.gov

If you or a partner agency utilize local LPRs, we encourage you to reach out to coordinate data share

Cari N. Schieno | Program Analyst

DEASIL | National License Plate Reader Program (LPR)
El Paso Intelligence Center (EPIC)
Desk: (571) 387-4220 | Cell: (915) [redacted]
Cari.N.Schieno@usdoj.gov

"Do right and fear not"

"We'd love to hear any success stories from you, the users. These justify the coverage and growth of this program!"
You can send your stories to LPR@usdoj.gov or to cari.n.schieno@usdoj.gov
Password/Account reset LPR@usdoj.gov

From: Hersey, Kevin <KCHersey@DEA.USDOJ.GOV>
Sent: Tuesday, April 21, 2020 3:26 PM
To: LPR <LPR@dea.usdoj.gov>
Subject: Re: SEAR-2020-03428 for Case #CZ-17-0025

Hi Cari-

Thank you for reaching out.
We did not utilize DEASIL, and I'm sorry to report that I have never been introduced to it.
In the current instance, a Mass State Police Trooper (TFO) entered our target vehicle into the LPR system in MA on our behalf and further alerted me to the notification.
I am interested in learning more about DEASIL and I will research it further.

Best regards,

Kevin Hersey
DEA New England Field Division
New Bedford Resident Office
617-[redacted] (cell)

On Apr 21, 2020, at 3:22 PM, LPR <LPR@dea.usdoj.gov> wrote:

> Hello SA Tenore and SA Hersey:
>
> I wanted to congratulate you on your recent successful mission! I am contacting you on behalf of the LPR program and I wondered, at your convenience, if you could confirm if you utilized DEASIL? If you did, would you be willing to share with us any additional information (I.E. seizure images and/or LPR hit) for DEASIL publications/training materials?

We greatly appreciate any and all input!
V/r

Cari N. Schieno | Program Analyst

DEASIL | National License Plate Reader Program (LPR)
El Paso Intelligence Center (EPIC)
Desk: (571) 387-4220 | Cell: (915) [redacted]
Cari.N.Schieno@usdoj.gov

"Do right and fear not"

"We'd love to hear any success stories from you, the users. These justify the coverage and growth of this program!"
You can send your stories to LPR@usdoj.gov or to cari.n.schieno@usdoj.gov
Password/Account reset LPR@usdoj.gov

From: Concorde_Notification_Service <Concorde_Notification_Service@dea.usdoj.gov>
Sent: Tuesday, April 21, 2020 10:25 AM
To: SEAR-New England <SEAR-NewEngland@dea.usdoj.gov>; CommandCenter-SEARS <CCSears@dea.usdoj.gov>; DEA.ONSI <DEAONSI@dea.usdoj.gov>; EPIC Bulk Currency SEARS Mailbox <EPIC.BulkCurrency.Se@dea.usdoj.gov>; NCWSEARS <NCWSEARS@dea.usdoj.gov>; ST - Emerging Technologies Support <TWG@dea.usdoj.gov>; SEAR-HQ <SEAR-HQ@dea.usdoj.gov>; DeLena, Jon C. <JCDeLena@DEA.USDOJ.GOV>; Bonner, Richard B. <rbbonner@dea.usdoj.gov>; Bonaventura Jr., Ronald <RBonaventura@dea.usdoj.gov>; Boyle, Brian D. <BDBoyle@DEA.USDOJ.GOV>; Belleau, Stephen P. <SPBelleau@dea.usdoj.gov>; Skeffington, Mark E. <MESkeffington@DEA.USDOJ.GOV>; Parrish, Lonnie L. <LLParrish@DEA.USDOJ.GOV>; Abraham Jr., Michael <MAbraham@dea.usdoj.gov>; Tenore, Louis (Jim) <LJTenore@DEA.USDOJ.GOV>; Desmond, Timothy <TJDesmond@DEA.USDOJ.GOV>; Morse, Asa C. <AXMorse@DEA.USDOJ.GOV>; Hersey, Kevin <KCHersey@DEA.USDOJ.GOV>; Angelucci, Albert P. <APAngelucci@DEA.USDOJ.GOV>; Lanzoni, David L. <DLLanzoni@DEA.USDOJ.GOV>; Krysil, Cara L <CLKrysil@dea.usdoj.gov>
Subject: SEAR-2020-03428 for Case #CZ-17-0025

Significant Enforcement Activity Report for Case #CZ-17-0025

SEAR Number: SEAR-2020-03428
Date of Submission: 4/21/2020
DEA Division: New England Field Division

From: Bender, Sean (POL)
To: Thibault, Amy (POL)
Cc: Smith, Eleanor (POL)
Subject: DRAFT - CFC Overview & Resources - NCO + LT Supervisor Training - January 2022
Date: Wednesday, December 29, 2021 10:04:00 AM
Attachments: DRAFT - Fusion Center Resources + Overview - DFS - SB.pptx
CFC Overview & Resources Training - Lesson Plan.docx

Good Morning, Amy -

Please find the attached *DRAFT - Fusion Center Overview & Resources (U//LES)* presentation and accompanying lesson plan, developed for the January/February 2022 Massachusetts State Police NCO + LT Supervisor Training(s), to be held on 1/4/2022, 1/11/2022, 1/25/2022, & 2/1/2022 at the Massachusetts State Police Academy (SPA) and/or Homeland Security Operations Center (HSOC).

For review, at your convenience.

It looks longer than it is at 28 slides, but it is very picture heavy and several slides are just contact information, etc. Rather than go in depth into each data source, I just want to be able to throw up a screenshot and describe in a couple sentences what information is available and maybe a couple hypothetical use cases. My objective is to give the class an awareness of what is *available to them* and how to request it, not make them experts.

1. Title Slide > Introduction > Contact Information > Hours of Operation
2. Workflow > Intake > Tactical Support (CFC Watch Center) + Strategic Support (CFC Maynard)
3. (U//LES) Disclaimer
4. CFC Mission Statement
5. Brief Overview of Fusion Centers (E.g. At least one in every state, CFC + BRIC in MA)
6. Overview of CFC Resources / Function
7. CJIS (Advanced Tools [Other than CJISWeb MSP 3.0])
8. CJIS > Brief Mention of AFIS-R
9. CJIS > Brief Mention of InmateWeb
10. CJIS > Brief Mention of InmateWeb (2nd Screenshot)
11. ACISS > Brief Mention of ACISS
12. Commercial Data Sources > CLEAR
13. Commercial Data Sources > TLO
14. Commercial Data Sources > ISO
15. Coplink > Brief Mention
16. ALPR > Brief Overview of Historical Data / Hotlists
17. OSINT > Brief Overview of OSINT Uses (Finding associates, etc)
18. Situational Awareness > SITREPS
19. Situational Awareness > Bulletins

20. PowerDMS > Intelligence Resources
21. Overview - SAR Indicators & Behaviors (1)
22. Overview - SAR Indicators & Behaviors (2)
23. Overview - SAR Indicators & Behaviors (3)
24. Special Event Support
25. INTERPOL
26. CCIP
27. MCP
28. Questions? > Contact Information (Again)

Let me know what you think? Once approved, I will forward Tpr. Paquette a copy of the signed Lesson Plan Cover Sheet for the Academy record.

Respectfully,

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

From: Terrey, Susan (EPS)
To: Staples, Jennifer (POL); Lord, Spencer (CDA)
Cc: Boyd, Donald A (EPS)
Subject: FW: 6/24 Joint Committee on Transportation - ALPR
Date: Friday, June 25, 2021 11:05:01 AM
Attachments: H.3597 & 3564 - Act Relative to License Plate Readers.docx
H.3609 – Act Relative to Unmanned Aerial Systems.docx

Jenn & Spence: Don a new member of our legal team attended the legislative hearing on the ALPR - see his notes below as well as his summaries of the bills. Let us know if you would like to discuss more.

From: Boyd, Donald A (EPS) <Donald.A.Boyd@mass.gov>
Sent: Friday, June 25, 2021 10:12 AM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Walker, Suleyken (EPS) <Suleyken.Walker@mass.gov>; Melander, John (EPS) <John.Melander@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: 6/24 Joint Committee on Transportation - ALPR

Good Morning!

The joint committee on transportation held a public hearing on ALPR regulations yesterday. Outlines for both ALPR bills along with the proposed Drone regulation are attached for reference. Highlights and comments of the hearing are listed below:

Public Comment

- Arline I. - Director of Mass. LGBTQI Political Group
    - Spoke in broad support of both ALPR bills
    - Expressed desire to regulate use of ALPR system to protect privacy of LGBTQI community so that an individual's movements are not specifically targeted by law enforcement for unlawful purposes (bias)
- ACLU
    - Spoke in support of H.3564
        - Less comprehensive bill of the two, does not create obligations specific to EPS as seen in H.3597
    - Believes **14 day data** retention cap is reasonable
    - Supports **warrant requirement** for law enforcement access to system
    - Reasoned that 16 states have adopted similar legislation including Maine and New Hampshire
        - ME ST T.29-A s. 2117-A
        - NH ST s. 261:75-b
- No comment by committee members
- No public or committee comment on H.3609 – Drone Regulation

Feel free to reach out with any follow-up questions!

-Don

From: Range, Scott (POL)
To: Kelley, David
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Friday, April 9, 2021 12:42:00 PM
Attachments: HIDTA_NCRIC CONOP MAY2020.docx
Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

From: Range, Scott (POL)
Sent: Monday, April 5, 2021 12:43 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, April 5, 2021 12:00 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law

enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is

accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle

information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do

so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Range, Scott (POL)
To: Range, Scott (POL)
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Monday, April 5, 2021 12:43:00 PM
Attachments: HIDTA_NCRIC CONOP MAY2020.docx
Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, April 5, 2021 12:00 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are

inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From:	Range, Scott (POL)
To:	Bender, Sean (POL)
Subject:	FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date:	Monday, April 5, 2021 11:53:37 AM
Attachments:	Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.pdf HIDTA_NCRIC CONOP MAY2020 (1).pdf

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or

a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses

the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence.

In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the

appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From:	Quinn, Dermot (POL)
To:	Range, Scott (POL)
Subject:	FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date:	Monday, March 8, 2021 2:53:13 PM
Attachments:	Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.pdf HIDTA_NCRIC CONOP MAY2020 (1).pdf

---

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS

Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

-

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various

federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history

information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC

personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Fallon, Jay
To: Quinn, Dermot (POL)
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Monday, March 8, 2021 2:11:32 PM
Attachments: Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.pdf
HIDTA_NCRIC CONOP MAY2020 (1).pdf

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

-

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide

them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to

comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a

secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Range, Scott (POL)
To: Kelley, David
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Friday, April 9, 2021 12:42:00 PM
Attachments: HIDTA_NCRIC CONOP MAY2020.docx
Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

From: Range, Scott (POL)
Sent: Monday, April 5, 2021 12:43 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Monday, April 5, 2021 12:00 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law

enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is

accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle

information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do

so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Donovan, Gerald (POL)
To: POL-DL-ICAC; POL-DL-DEMS
Subject: Fw: Emailing: MDEG Second Version 062021
Date: Thursday, June 24, 2021 12:40:08 PM
Attachments: MDEG Second Version 062021.pdf

I might have missed this, but just in case no one else received it.

Respectfully,

Trooper Jerry Donovan, #3424
Massachusetts State Police
Cyber Crime Unit
Internet Crimes Against Children Task Force
50 Maple St, Milford, MA 01757
W: (774) 462-3750
Gerald.Donovan@pol.state.ma.us

From: Lavoie, Matt (CPI) <matt.lavoie@mass.gov>
Sent: Thursday, June 24, 2021 12:21 PM
To: Donovan, Gerald (POL) <gerald.donovan@pol.state.ma.us>
Subject: Emailing: MDEG Second Version 062021

Your message is ready to be sent with the following file or link attachments:

MDEG Second Version 062021

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

From:	Wilcox, Christopher (POL)
To:	Egnitz, Brian (POL)
Subject:	FW: License Plate Reader Program Best Practices Guide.
Date:	Friday, November 12, 2021 10:04:00 AM
Attachments:	LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

Brian – Some great stuff in here

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, November 12, 2021 9:11 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: License Plate Reader Program Best Practices Guide.

Sir,
Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From:	Wilcox, Christopher (POL)
To:	Pack, Noah (POL)
Subject:	FW: License Plate Reader Program Best Practices Guide.
Date:	Friday, November 12, 2021 9:38:00 AM
Attachments:	LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, November 12, 2021 9:11 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: License Plate Reader Program Best Practices Guide.

Sir,
Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From:	Wilcox, Christopher (POL)
To:	Scott, Michael (POL)
Subject:	FW: License Plate Reader Program Best Practices Guide.
Date:	Friday, November 12, 2021 10:04:00 AM
Attachments:	LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Friday, November 12, 2021 9:11 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: License Plate Reader Program Best Practices Guide.

Sir,
Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From:	Brooks, Brian (POL)
To:	Bender, Sean (POL)
Subject:	FW: LPR"s
Date:	Tuesday, November 2, 2021 10:59:00 AM
Attachments:	LicensePlateReaderProgramBestPracticesGuide-October2021.pdf image002.png

---

From: Boyle, Christopher (DOT) <Christopher.P.Boyle@dot.state.ma.us>
Sent: Tuesday, November 2, 2021 10:49 AM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>
Subject: LPR's

Sirs,

AAMVA is the American Association of Motor Vehicle Administrators. It is a private organization that almost every RMV/DMV is part of.

They just released the License Plate Reader Program Best Practices Guide.

I have attached it if it can be of assistance.

Respectfully,

Chris

Lieutenant Christopher Boyle #2710
Massachusetts State Police
Division of Homeland Security and Preparedness
Fraud Identification Unit
185 Kneeland St., 5th Floor
Boston, MA 02111
christopher.boyle@mass.gov
cell: 781-[redacted]

From: Egnitz, Brian (POL)
To: Pack, Noah (POL)
Subject: FW: Massachusetts State Police ALPR - Verizon Mobile Private Network
Date: Monday, November 22, 2021 2:01:00 PM
Attachments: MSP- ALPR Private Network Options 03 01 2021.pdf

---

From: Jussaume, Carolyn B <carolyn.jussaume@verizonwireless.com>
Sent: Monday, March 1, 2021 9:34 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Michael Caralis <michael.caralis@verizonwireless.com>; Paul Ralston <paul.ralston@verizonwireless.com>; Marshall Roger <roger.marshall@verizonwireless.com>; William M Reed <william.reed1@one.verizon.com>; Nugent, Michael (Data Sales) <michael.nugent@verizonwireless.com>; Borell, Ben <Ben.Borell@verizonwireless.com>
Subject: Re: Massachusetts State Police ALPR - Verizon Mobile Private Network

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

Lt Colonel Quinn and Brian

Attached is a high level summary of each option with the associated costs from Verizon. Pls also check out the documents that Ben provided, as they provide a more thorough private network explanation. We did make some assumptions about the amount of bandwidth needed for the Secure Cloud Interconnect option not really knowing the projected data needs at this point (this can be fine tuned once more information is available). As we mentioned, Verizon does have professional services which can assist in many areas- if there are some areas that MSP would like assistance, pls let us know and we can put together a statement of work and a quote for that as well.

Please let us know if you would like to set up some time to review the information.

Carolyn

On Thu, Feb 25, 2021 at 10:27 AM Borell, Benjamin <ben.borell@verizonwireless.com> wrote:

> Good Morning,
>
> Following up on our conversation from the other day, attached are a few documents:
>
> - A Verizon Mobile Private Network (MPN) whitepaper
> - A PDF diagram of proposed design options for LTE routers to reach AWS
> - A Word document that would be used to collect customer network inputs for an MPN using IPSec VPN over the Internet.

- I have highlighted some key sections of the form and have also made some notes in *Comic Sans* font to clarify what VZ is seeking in that particular section.
- If the decision is reached by MSP to utilize Secure Cloud Interconnect I would provide a similar, but slightly different form which does not require inputs for VPN tunnels.

We'd be happy to set up a web call to review one or both private network intake forms. I will defer to Carolyn, Paul, and William to provide pricing for the two design options.

Lastly, both design options are supported by the Verizon Wireless Help Desk (WEHD) which offers 24x7x365 tier two tech support for Mobile Private Network projects.

Thank you,
Ben



Benjamin Borell

Sr. Solutions Engineer
Field Pre-Sales Engineering
Verizon Business Group

M 617 872 8330

--



Carolyn Jussaume

Business Development
Massachusetts Government Team
Verizon Business Group

M 617 699 3900
1 Washington Mall, 6th Floor
Boston, Massachusetts 02109



From: Pack, Noah (POL)
Subject: Fw: MOU Contacts
Date: Wednesday, December 15, 2021 9:48:00 AM
Attachments: image001.png
image002.png
image003.png
BCPO+Law+Enforcement+Directive+No.+2020-10+with+Attachments.pdf
Post Falls Idaho PD ALPR MOU-04202021.pdf

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, December 14, 2021 2:47 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: MOU Contacts

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

Great,

I've been waiting on some customers for MOU's that you had asked for. Not to delay any further I've attached two that I've received so far for your review.

For contacts: John Mittmann -IT Administrator jmittmann@postfallspolice.com; (208) 773-3517 of Post Falls Police and Brian Rodriques -Asst Deputy Director brodriques@ncric.ca.gov; (415) 710-9702 of The Northern California Regional Intelligence Center are fairly large user of ours.

Regards,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, December 14, 2021 10:58 AM
To: John Tedona <jtedona@neology.net>
Subject: Re: Wednesday 1PM Meeting

Hi John,

That's fine with me. There is a TV available in our conference room.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Monday, December 13, 2021 9:56 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Wednesday 1PM Meeting

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

Hi Noah,

I'd like to have Bob Fecteau and Kory Koster of BCM Controls join us in Wednesday's meeting if that's okay with you. This way you will have representation of the manufacture (me), the sales side (Bob Fecteau) and the on-site support technician (Kory Koster) in the meeting to cover any questions that you may have.

I'll have my ALPR demonstration vehicle so I can provide a live mobile ALPR demo. To provide an overview of BOSS4 will a large monitor be available that I could connect with my laptop for easier viewing?

Thanks,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

From:	Wilcox, Christopher (POL)
To:	Warren, Rosemary (POL)
Subject:	FW: postings
Date:	Friday, September 10, 2021 9:57:00 AM
Attachments:	National_ANPR_Service_technical_specifications.pdf National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version) - GOV.UK.pdf NASPLE_Version_2.1_November_2020.pdf

---

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, September 9, 2021 5:51 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: RE: postings

Here are a bunch of ideas for your consideration. Let me know when you can review and I can add context. It's a mix of tasks that would need to be simplified for a posting. I've also included some good docs that we could borrow from.

-Brian

ALPR coordinator will:

- Work to establish a new MSP ALPR Program
- facilitate ALPR data sharing thought public safety in the public safety community
- Manage MSP Commercial ALPR Vendor accounts, such as Vigilant National plate reader database, or new systems offered to MSP like Flock
- Track trends in ALPR technology
- Track legal rulings and advise
- Maintain a list of known ALPR systems used by Public Safety (including Department, system type, technology used, retention period and contacts)
- Provide support to MSP and Local Departments in use or purchase of ALPR technology as requested
- Facilitate sharing of Hotlists to disparate systems for Amber or related significant events
- Maintain hotlist compliance (Case number, cause and removal in timely manner)
- Perform advanced ALPR searches (such as convoy or cohort)
- Maintain Regional Hotlist / WMS Alert system
- Become POC for MassTurn Pike exigency requests (not sure who does this now)
- Establish a ALPR minimum data standard for new Equipment
- Administer the Agency ALPR system
- Perform system and hotlist audits
- Monitor system and report issues or outages to appropriate personnel
- Manage user accounts and permissions
- Interact with ALPR vendor(s)
- Identify best practices
- Provide user training
- Provide expert witness testimony

- Maintain success stores
- Monitor cloud subscription for overages
- Perform ad-hoc and statistical reporting
- Respond to legal process and public record requests
- Work with MSP / EOPSS Legal to create data sharing agreements with contributing agencies.
    - To Include data standards and audit requirements for all submitting Agencies
- Work with MSP / EOPSS Legal to execute cloud agreement with MSP ALPR vendor [Neology] (see DCJIS template)
- Work with MSP / EOPSS Legal to execute agreement with 3rd party ALPR vendors (such as Flock or Vigilant)
- Seek grants for replacing equipment
- Work with Fiscal to budget for replacement equipment
- Coordinate new ALPR camera purchases, such as the Truck Teams new purchase to maintain compliant equipment
- Work with TSS/EOPSS/MSP to migrate preserved data
- Work with TSS/EOPSS/MSP to migrate existing cameras to the new Cloud solution
- Work with TSS/EOPSS/MSP to migrate hot file connections to cloud
- Work with TSS/EOPSS/MSP to migrate decommission EOPSS BOSS 3.6

Desired experience

- Existing subject matter expert in ALPR technology
- Experience in use of or application of ALPR technology
- Proficient in use of web based technologies
- Experience in managing applications and permissions

From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Sent: Thursday, September 9, 2021 12:41 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: postings

Brian - Can you get me a couple of bullets for LPR Coordinator?

Lieutenant Colonel Christopher T. Wilcox

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Road

Framingham, MA 01702

From: Wilcox, Christopher (POL)
To: Warren, Rosemary (POL)
Subject: Fw: postings
Date: Wednesday, November 10, 2021 3:27:40 PM
Attachments: ALPR Coordinator Posting - Sergeant - September 2021.docx

---

Lieutenant Colonel Christopher T. Wilcox
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road
Framingham, MA 01702

508 820-7301

From: Wilcox, Christopher (POL)
Sent: Friday, September 10, 2021 11:42 AM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Subject: FW: postings

From: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Sent: Friday, September 10, 2021 11:20 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: RE: postings

LTC,

Please take a look at this first DRAFT

Respectfully,

Rose

Rosemary J. Warren
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Office: 508-988-7310
Rosemary.Warren@mass.gov

From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Sent: Friday, September 10, 2021 9:57 AM
To: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Subject: FW: postings

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, September 9, 2021 5:51 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: RE: postings

Here are a bunch of ideas for your consideration. Let me know when you can review and I can add context. It's a mix of tasks that would need to be simplified for a posting. I've also included some good docs that we could borrow from.

-Brian

ALPR coordinator will:

- Work to establish a new MSP ALPR Program
- facilitate ALPR data sharing thought public safety in the public safety community
- Manage MSP Commercial ALPR Vendor accounts, such as Vigilant National plate reader database, or new systems offered to MSP like Flock
- Track trends in ALPR technology
- Track legal rulings and advise
- Maintain a list of known ALPR systems used by Public Safety (including Department, system type, technology used, retention period and contacts)
- Provide support to MSP and Local Departments in use or purchase of ALPR technology as requested
- Facilitate sharing of Hotlists to disparate systems for Amber or related significant events
- Maintain hotlist compliance (Case number, cause and removal in timely manner)
- Perform advanced ALPR searches (such as convoy or cohort)
- Maintain Regional Hotlist / WMS Alert system
- Become POC for MassTurn Pike exigency requests (not sure who does this now)
- Establish a ALPR minimum data standard for new Equipment
- Administer the Agency ALPR system
- Perform system and hotlist audits
- Monitor system and report issues or outages to appropriate personnel
- Manage user accounts and permissions
- Interact with ALPR vendor(s)
- Identify best practices
- Provide user training
- Provide expert witness testimony
- Maintain success stores
- Monitor cloud subscription for overages
- Perform ad-hoc and statistical reporting
- Respond to legal process and public record requests
- Work with MSP / EOPSS Legal to create data sharing agreements with contributing agencies.

    - To Include data standards and audit requirements for all submitting Agencies
- Work with MSP / EOPSS Legal to execute cloud agreement with MSP ALPR vendor [Neology] (see DCJIS template)
- Work with MSP / EOPSS Legal to execute agreement with 3rd party ALPR vendors (such as Flock or Vigilant)
- Seek grants for replacing equipment
- Work with Fiscal to budget for replacement equipment
- Coordinate new ALPR camera purchases, such as the Truck Teams new purchase to maintain compliant equipment
- Work with TSS/EOPSS/MSP to migrate preserved data
- Work with TSS/EOPSS/MSP to migrate existing cameras to the new Cloud solution
- Work with TSS/EOPSS/MSP to migrate hot file connections to cloud
- Work with TSS/EOPSS/MSP to migrate decommission EOPSS BOSS 3.6

Desired experience

- Existing subject matter expert in ALPR technology
- Experience in use of or application of ALPR technology
- Proficient in use of web based technologies
- Experience in managing applications and permissions

From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Sent: Thursday, September 9, 2021 12:41 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: postings

Brian - Can you get me a couple of bullets for LPR Coordinator?

Lieutenant Colonel Christopher T. Wilcox
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road
Framingham, MA 01702

508 820-7301

From: Bender, Sean (POL)
To: Thibault, Amy (POL)
Subject: Fw: Promulgation of 19-SO-12
Date: Thursday, March 18, 2021 7:44:43 AM
Attachments: 19-SO-12 Distribution of General Order.pdf
TRF-11 Automatic License Plate Recognition Revised 10-1-2019 with highlights.pdf

---

Applicable RE: Vigilant?

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

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, November 12, 2019 10:47 AM
To: McCarthy, Daniel (POL) <Daniel.McCarthy@pol.state.ma.us>
Cc: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: Fw: Promulgation of 19-SO-12

From: Strategic Planning (POL) <strategic.planning@massgov.onmicrosoft.com>
Sent: Tuesday, October 1, 2019 5:20 PM
To: POL-DL-All Users <POL-DL-AllUsers@MassMail.State.MA.US>
Subject: Promulgation of 19-SO-12

Please be advised that the following Special Order has been promulgated:

- **19-SO-12 Distribution of General Order**
  TRF-11 Automatic License Plate Recognition

Please also be advised that the official General Order listed in the above Special Order has been promulgated.

Strategic Planning Section
470 Worcester Road
Framingham, Massachusetts 01702

From: Fitzge a d Thomas (POL)
Subject: Fw: Proposed Reg/Statute updates to c. 90 or FAST Act compl ance
Date: Monday April 5 2021 4:18:10 PM
Attachments: 00 CMR 7 Redl ne.doc
Redl ne to c 90 Sect on 1 - de init ons.doc
Redl ne to c 90 Sect on 19A.doc
Redl ne to G L c 90 Section 19.doc
Redl ne to G L c 90 Section 19F.doc
RE Pro osed dates to c 90 or FAST Act com l ance.msg

From Osborne Chester (DOT) <Chester.Osborne@dot state.ma.us>
Sent Monday April 5 2021 15 22
To Myslinski Tara (DOT)
Cc DelVento Anthony J. (DOT) Fanning Jessica M. (DOT) Fitzgerald Thomas (POL) Rizzuto Elizabeth (DOT) N les Makaela (DOT) Lee Donna M. (DOT) Weidele Matthew (DOT) Bardow Alexander K. (DOT) Slack Just n (DOT)
Subject FW Proposed Reg/Statute updates to c. 90 for FAST Act compliance

Hello all. As many of you know Ms. Myslinski has been working hard to updated the regs around commercial ehicles and frieght. These latest drafts (a tached) represent he culmination of many months of work drafts and re isions to support this line of effort. We now find oursel es at the last draft and facing the deadline to mo e th s up the chain.

Please take some time to re iew the attached and below prior o Thursday of his week. If you need to make edits please use track changes in the doc and rename it wi h your stakeholder group in the file name and send it back to Ms. Myslinski and CC myself no later than COB Thursday 8 h. If you ha e no comments or edits and affirmation of same is appreciated.

In a moment I w ll send a calendar in ite for 11am Thursday the 8th this is by no means a mandatory mee ing for anyone in fact it is really more of "office hours" in case you need to ha e a con ersation around any feedback and to conduct any joint editing exercises.

When making re iew please consider any limitations for the MHS Tunnels Bridges or other unique situations. As well as inform as to any other rules policies or procedures that these proposed changes could impact. Last feel free to include any stakeholders or members of your team that I may ha e missed. Thank you for your support in his matter.
V/r Chet.

Ches er Osborne
Dir. of TSMO
617.719 5 77

From Myslinski Tara (DOT) <Tara.Myslinski@dot state.ma.us>
Sent Monday April 5 2021 2 57 PM
To Osborne Ches er (DOT) <Chester.Osborne@dot.state.ma.us>
Cc Fenton Eileen (DOT) <Eileen.Fenton@dot.state.ma us>
Subject Proposed Reg/Statute updates to c. 90 for FAST Act compliance
Importance High

Chet the attached redlines of current sta utes and regs are ready for re iew by the FOG. I added a couple of items based on Chris's feedback. You may also want o send the FOG Chris's email and/or the link to the FAST Act pro isions that Chris sent (attached and below for con enience) unless you hink that would confuse the re ew – hat is up to you.

ht ps://ops fhwa.dot.go freight/pol plng finance/policy/fas act/twopro isions/index.htm#description<https://urldefense.com/ 3/ https /ops.fhwa do go /freight/pol plng finance/pol cy fastact/twopro isions/index.htm*description Iw!!CUhgOOZgV7M!3V0RGH1tjCKZFl xErsVE0Rif1qU5JjzdnpKrfcCo 1JgMnkK3PsDhGiD7wjFxOXKmUNCk$>

If we are going to submit these legislati e changes as part of he Go ernor's safety bill we need the language by April 12 – a week from today. Do you th nk we could get comments this week? Happy to meet and discuss.

Tara Myslinski
Senior Lead Counsel Regulatory & Compliance
MassDOT
Ten Park Plaza Suite 3510
Boston Massachuse ts 02116
Mobile 857-360-6810
Tara.myslinsk @dot state.ma.us<mailto:T y l @ >

[image003]

MassDOT and the MBTA are subject to MGL Chpt.66 Sec.10 Public Records Law. Email sent or recei ed by MassDOT and MBTA employees are subject to these laws. Unless otherw se exempted from the public records law senders and recei ers of MassDOT and MBTA email should presume that the email are sub ect to release upon request and to state record retention requirements.

Conf dentiality No ice [This communication (includ ng any attachments) is only intended for the user of the indi idual or entity to which t is directed. It may conta n information that is pri ileged confidential and exempt from disclosure under applicable law and should not be read cop ed or o herwise used by any other person. If recei ed in error please notify he sender immediately and delete the e-mail and any attachment(s) from your system without copying forwarding disclos ng or using it n any other way.

From: Lavoie, Matt (CPI)
To: Barnard, Diana (CPI); Cosgrove, Richard (CPI); Diotte, Jeffrey (POL); Dunphy, David (POL); Fries, Joshua (POL); Furtado, Gregory (POL); Hanafin, John (CPI); Lavoie, Matt (CPI); Macdonald, Paul (POL); McCabe, Scott (CPI); Perkins, Taylor (CPI); Porter, Bradford (POL); Powell, Marc S (POL); Shaw, Dustin (POL); Ungechauer, Stan J (POL); Gregg, Theodore (POL); Walczak, David J (POL); Waskiewicz, Justin J (POL)
Subject: FW: The Massachusetts Digital Evidence Guide June 2021
Date: Wednesday, June 16, 2021 3:33:25 PM
Attachments: MDEG Second Version 062021.pdf

Attached is the updated Digital Evidence guide put out by the AG's office. It covers the search and seizer of pretty much any type of digital evidence and should answer any questions on search warrant issues. I also saved it on the Q-Drive under CSLI-Ping folder.

Sergeant Matthew R. Lavoie #3138
Massachusetts State Police Detetive Unit
Cape Cod & the Islands
Office: (508) 790-5799

-----Original Message-----
From: mdec@listserv riss net <mdec@listserv.riss net>
Sent: Tuesday, June 1, 2021 4:34 PM
To: mdec@listserv.riss.net
Subject: The Massachusetts Digital Evidence Guide June 2021

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

Good Afternoon Everyone,

Attached, please find the second version of the Massachusetts Digital Evidence Guide, June 2021 edition. It is updated with cases issued through early this year. The MDEG first edition was issued in June of 2015, a resource and vision of the Cyber Crime Division of the AGO, and particularly CCD Chief Tom Ralph, who now serves as Chief of the Middlesex Appeals Division and active MDEC Member. The first edition was cited to in more than one decision from Massachusetts courts, including the SJC in the 2017 case Commonwealth v. Molina. In Molina, the SJC stated, "The Attorney General's existing digital evidence guide offers helpful parameters, and we invite the Attorney General to develop further guidance for the conduct of digital searches that could be made available to both State and local officers conducting digital searches." In short, this MDEG has proved to be an invaluable resource for many over the course of the years. One of the ways we have continued to address this specific concern from the SJC are the continued training and outreach initiatives of MDEC.

Starting with Dorelas in 2016, our Appeals Courts have issued dozens of impact cases on digital evidence. So many in fact that keeping up with updates to the MDEG has been very difficult. Remarkably enough, we already have several cases to add since the attached version was finalized. Regardless, it is here. Many of you helped contribute thoughts and submissions a few years ago. Lots of legal interns - and a partnership with the AGO Appeals Division - helped push it over the finish line. Thank you to all, including AGO Appeals Division Chief Randy Ravitz and Deputy Division Chief Tom Bocian and AAsG Maria Granik and Anna Lumelsky, for the contributions of time, effort, and expertise to this important initiative.

Please email me with any questions or if you notice anything that needs to be adjusted. We have stared at this endlessly for long periods of time. Mark Twain wisely said, "continued progress is better than delayed perfection." So this resource will continue to be a work in progress. Every police officer and prosecutor in Massachusetts can

benefit from the time investment.

-CK

_____

Christopher W. Kelly
Director
Digital Evidence Laboratory
Commonwealth of Massachusetts
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
617.963.2146 (office)
617.963.2620 (lab main)
christopher kelly@mass.gov

This e-mail, including attachments, may contain confidential or privileged information and is solely for the use of the intended recipient. If you have received this communication in error, please notify the sender immediately and delete this message from your system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

##############################
This message is sent to you because you are subscribed to the mailing list mdec@listserv.riss.net.
To unsubscribe, E-mail to: mdec-off@listserv.riss.net

Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, forwarding or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Any information that is disseminated via listserv riss net is considered property of the issuing agency.

From: Craig Lynch
To: Pack, Noah (POL)
Subject: Fwd: MOU and Axon Promo - Flock Safety
Date: Tuesday, December 7, 2021 9:51:10 PM
Attachments: NPF LPR Study Brief_11-15-2021.pdf

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

Sgt - Please see the response below and the attachment. Do you have some time to talk this week?

Craig

---------- Forwarded message ---------
From: **Bob Carter** <bob.carter@flocksafety.com>
Date: Tue, Dec 7, 2021 at 9:38 PM
Subject: Re: MOU and Axon Promo - Flock Safety
To: Craig Lynch <craig.lynch@flocksafety.com>

The LPR database is controlled and owned by the PD. NPF will not have access to this. The data is statistical analysis. The attached document provides more information. Please set up a call with the three of us to discuss.

Bob Carter
Director, Strategic Alliances
Flock Safety
404-631-6317 | bob.carter@flocksafety.com

On Tue, Dec 7, 2021 at 9:33 PM Craig Lynch <craig.lynch@flocksafety.com> wrote:

> Mr Bob - Mass State Police is interested in the Axon free cams . Any insight on the email below?
>
> ---------- Forwarded message ---------
> From: **Pack, Noah (POL)** <noah.pack@state.ma.us>
> Date: Tue, Dec 7, 2021 at 9:04 PM
> Subject: Re: MOU and Axon Promo - Flock Safety
> To: Craig Lynch <craig.lynch@flocksafety.com>
>
> Hi Craig,
>
> I am setting up a meeting with our legal section regarding a number of issues, to include the Flock MOU and nationwide study/trial program. I expect to be asked for the fine print on the

study, including what are we expected to do with our participation, what happens to the data, etc. Can you provide any further info on that?

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: Craig Lynch <craig.lynch@flocksafety.com>
Sent: Wednesday, December 1, 2021 9:16 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: MOU and Axon Promo - Flock Safety

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

Sgt Pack - Nice speaking with you this morning. I have attached the Flock Safety MOU which will give access to everything in the system as a paying custom other than the NationWide Search of ~9500 cameras.

Below is the email with details on the Axon promotion. It's a bit lengthy, but 1 year, no obligation, no multi-year commitment.

As Axon Founder and CEO Rick Smith announced at the MCSA Fall Meeting, Axon along with its partner Flock Safety, will provide all MCSA agencies Automated License Plate Readers (ALPR) for one year for those willing to participate in a national study conducted by the Police Foundation. While many recognize the crime-reduction benefits of ALPR technology, questions have been raised about how effective they are at reducing all crime types as well the civil liberties and privacy implications of this technology. This study will attempt to provide a robust research design and methodology to address those questions and concerns.

If your agency is willing to take part in this national study, you will receive:

- **25 Flock Safety ALPRs for 1 year, which includes the ALPR readers, solar or DC power, mounting equipment, and installation.**
- **This also includes all cloud hosting and analytics, including LTE connectivity,**

unlimited licenses, hotlist integration and alerts, and ongoing software enhancements.

- **Flock Safety will make their SMEs available to assist agencies with identifying the most effective ALPR locations.**
- **Agencies can purchase additional cameras beyond the 25. Axon and Flock will cover the installation costs of these additional cameras.**
- **This offer applies to any MCSA agency, including those that have already purchased Flock ALPRs.**
- **After the 1-year field trial offer ends, each agency has the option to purchase the units at $2500 per year per ALPR.**
- **Should an agency choose not to retain the ALPRs after the field trial, we will ensure that the agency is able to transfer their data to another system and we will remove the ALPRs at no cost to the agency.**

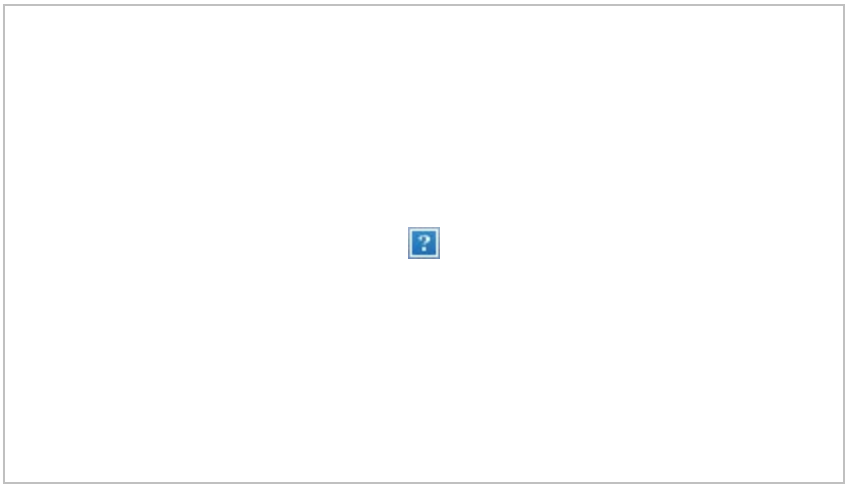
In addition, we understand that across the country there are varying laws and regulations about ALPR technology. Axon's Government Affairs team will be available to your agency to provide an overview of any state and county ALPR laws that are applicable. We will also provide model ALPR policies to your agency prior to deployment. And, our Government Affairs team can act as a resource to meet with and educate any county board member(s) on Axon, Flock Safety, ALPR technology — and our ethics-first design philosophy.

If you or your team have any questions, please let me know.

Thanks for your partnership,

Craig

--



This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s).

From: Cyr, Mark (POL)
To: Wilcox, Christopher (POL)
Subject: License Plate Reader Program Best Practices Guide.
Date: Friday, November 12, 2021 9:10:40 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

---

Sir,

Per our conversation on Wednesday...

Mark

Major Mark D. Cyr #2728
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
978-451-3773 (office)
508-[redacted] (cell)

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

From: Wilcox, Christopher (POL)
To: Benincasa, Jeanne (EPS)
Subject: LPR Article
Date: Friday, December 3, 2021 10:01:00 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf

---

Undersecretary Benincasa – I attached a document about best practices for LPR Programs. It's very informative, and I felt Chapter 7 "LPR Success stories" was interesting. CTW

Lieutenant Colonel Christopher T. Wilcox
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Road
Framingham, MA 01702

508 820-7301

From: Boyle, Christopher (DOT)
To: Cyr, Mark (POL); Tucker, Daniel T (POL); Brooks, Brian (POL); O"Hara, Edward (POL)
Subject: LPR"s
Date: Tuesday, November 2, 2021 10:48:35 AM
Attachments: LicensePlateReaderProgramBestPracticesGuide-October2021.pdf
image002.png

Sirs,

AAMVA is the American Association of Motor Vehicle Administrators. It is a private organization that almost every RMV/DMV is part of.

They just released the License Plate Reader Program Best Practices Guide.

I have attached it if it can be of assistance.

Respectfully,

Chris

Lieutenant Christopher Boyle #2710
Massachusetts State Police
Division of Homeland Security and Preparedness
Fraud Identification Unit
185 Kneeland St., 5th Floor
Boston, MA 02111
christopher.boyle@mass.gov
cell: 781-[redacted] G.L. c. 4 sec. 7 cl.26 (n)(s



To:	Wilcox, Christopher (POL)
Cc:	Egnitz, Brian (POL)
Date:	Monday, November 22, 2021 2:41:05 PM
Attachments:	MSP- ALPR Private Network Options 03 01 2021.pdf Pricing Proposal- BCM Controls_Sierra MP70 Routers, Accessories & ALMS Through June 30, 2022 REV1 10012021.pdf Pricing Proposal- BCM Controls_Sierra MP70 Routers, Accessories & ALMS Through June 30, 2023 REV1 10012021.pdf

---

Lieutenant Colonel Wilcox,

Please see the attached TFL and cost proposals for equipment and services that are necessary for the upgrade and maintenance of the Department's ALPR network.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona
To: Pack, Noah (POL)
Subject: Mobile Training
Date: Friday, December 10, 2021 11:57:19 AM
Attachments: image001.png
image002.png
image003.png
PAGIS 2.14 MANUAL_ADMIN.pdf
PAGIS 2.14 MANUAL_USERS.pdf

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

Noah,

I've attached the latest training PDFs for our mobile ALPR systems. A new version will be available soon that will include the NTP time server lock water mark on the vehicle over view and license plate images.

Regards,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Craig Lynch
To: Pack, Noah (POL)
Subject: MOU and Axon Promo - Flock Safety
Date: Wednesday, December 1, 2021 9:17:13 AM
Attachments: MA Massachusetts State PD - MOU.pdf

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

Sgt Pack - Nice speaking with you this morning. I have attached the Flock Safety MOU which will give access to everything in the system as a paying custom other than the NationWide Search of ~9500 cameras.

Below is the email with details on the Axon promotion. It's a bit lengthy, but 1 year, no obligation, no multi-year commitment.

As Axon Founder and CEO Rick Smith announced at the MCSA Fall Meeting, Axon along with its partner Flock Safety, will provide all MCSA agencies Automated License Plate Readers (ALPR) for one year for those willing to participate in a national study conducted by the Police Foundation. While many recognize the crime-reduction benefits of ALPR technology, questions have been raised about how effective they are at reducing all crime types as well the civil liberties and privacy implications of this technology. This study will attempt to provide a robust research design and methodology to address those questions and concerns.

If your agency is willing to take part in this national study, you will receive:

- **25 Flock Safety ALPRs for 1 year, which includes the ALPR readers, solar or DC power, mounting equipment, and installation.**
- **This also includes all cloud hosting and analytics, including LTE connectivity, unlimited licenses, hotlist integration and alerts, and ongoing software enhancements.**
- **Flock Safety will make their SMEs available to assist agencies with identifying the most effective ALPR locations.**
- **Agencies can purchase additional cameras beyond the 25. Axon and Flock will cover the installation costs of these additional cameras.**
- **This offer applies to any MCSA agency, including those that have already purchased Flock ALPRs.**
- **After the 1-year field trial offer ends, each agency has the option to purchase the units at $2500 per year per ALPR.**
- **Should an agency choose not to retain the ALPRs after the field trial, we will ensure that the agency is able to transfer their data to another system and we will remove the ALPRs at no cost to the agency.**

In addition, we understand that across the country there are varying laws and regulations about ALPR technology. Axon's Government Affairs team will be available to your agency to provide an overview of any state and county ALPR laws that are applicable. We will also provide model ALPR policies to your agency prior to deployment. And, our Government

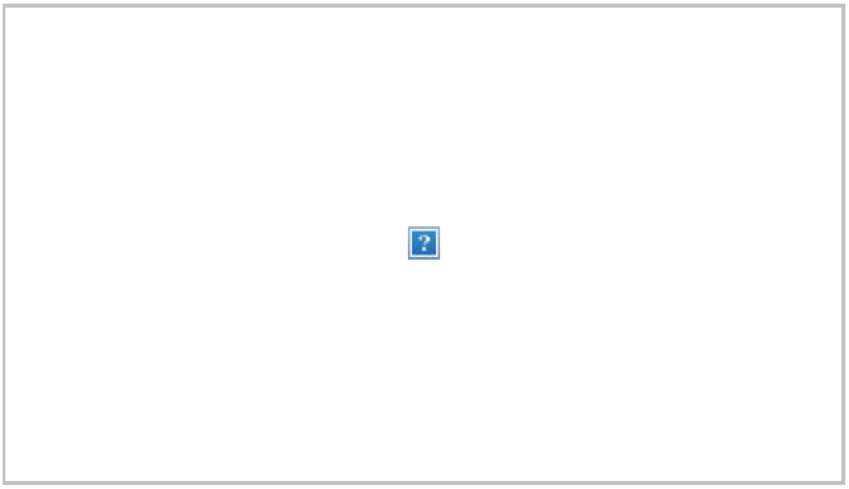
Affairs team can act as a resource to meet with and educate any county board member(s) on Axon, Flock Safety, ALPR technology — and our ethics-first design philosophy.

If you or your team have any questions, please let me know.

Thanks for your partnership,

Craig

--



From: John Tedona
To: Pack, Noah (POL)
Subject: MOU Contacts
Date: Tuesday, December 14, 2021 2:49:00 PM
Attachments: image001.png
image002.png
image003.png
BCPO+Law+Enforcement+Directive+No.+2020-10+with+Attachments.pdf
Post Falls Idaho PD ALPR MOU-04202021.pdf

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

Great,

I've been waiting on some customers for MOU's that you had asked for. Not to delay any further I've attached two that I've received so far for your review.

For contacts: John Mittmann -IT Administrator jmittmann@postfallspolice.com; (208) 773-3517 of Post Falls Police and Brian Rodriques -Asst Deputy Director brodriques@ncric.ca.gov; (415) 710-9702 of The Northern California Regional Intelligence Center are fairly large user of ours.

Regards,

neology
mobility [re]imagined

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Tuesday, December 14, 2021 10:58 AM
To: John Tedona <jtedona@neology.net>
Subject: Re: Wednesday 1PM Meeting

Hi John,

That's fine with me. There is a TV available in our conference room.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Monday, December 13, 2021 9:56 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Wednesday 1PM Meeting

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

Hi Noah,

I'd like to have Bob Fecteau and Kory Koster of BCM Controls join us in Wednesday's meeting if that's okay with you. This way you will have representation of the manufacture (me), the sales side (Bob Fecteau) and the on-site support technician (Kory Koster) in the meeting to cover any questions that you may have.

I'll have my ALPR demonstration vehicle so I can provide a live mobile ALPR demo. To provide an overview of BOSS4 will a large monitor be available that I could connect with my laptop for easier viewing?

Thanks,

neology
mobility [re]imagined

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

From: Enrique Cramer
To: Sharon Easley (seasley@e-squared.org)
Cc: Fitzgerald, Thomas (POL)
Subject: MSP Smart Roadside Trailer - Extended Support & Maintenance Services
Date: Friday, October 1, 2021 12:23:27 PM
Attachments: Q2021851_MA_SP_IIS_Support_Maintenance_Services_(SMS)_Plan_Oct_1_2021.pdf

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

Hi Sharon,

As per our recent call, the extended support & maintenance services (SMS) for MA State Police Smartroadside Trailer expired yesterday.
Lt. Fitzgerald confirmed that they would like to extend SMS thus here is a quote for the next 3 years.

FYI – Previously, SMS for the trailer flowed through "Access Control Systems, Inc" who have a statewide contract with MSP. Moving forward, SMS will go directly through IIS.
Let me know if we need to do anything on our end (i.e. register as a vendor) to support this.

Cheers,

Enrique
778.384.4341

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series Today at 1:00 pm EST: CODY Systems
Date: Wednesday, May 12, 2021 9:16:55 AM
Attachments: May Calendar.pdf

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

Today's Sponsor Education Series presentation is hosted CODY Systems. Session information and a registration link are below. Also attached is the May Sponsor Education Series calendar.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data fusion technology fuels fusion centers with a one-stop search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider.

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Thank you for participating in the NFCA Sponsor Education Series.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series Today at 1:00 pm EST: CODY Systems
Date: Wednesday, May 12, 2021 9:11:06 AM
Attachments: May Calendar.pdf

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

Today's Sponsor Education Series presentation is hosted CODY Systems. Session information and a registration link are below. Also attached is the May Sponsor Education Series calendar.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data fusion technology fuels fusion centers with a one-stop search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider.

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Thank you for participating in the NFCA Sponsor Education Series.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series - May Calendar with Updated Links
Date: Tuesday, May 11, 2021 11:52:47 AM
Attachments: May Calendar.pdf

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

Good morning,

An update to the May NFCA Sponsor Education Series is attached. Several revised links are provided.

The Sponsor Education Series kicks off tomorrow (Wednesday, May 11) at 1:00 pm EST with a 30 minute webinar presented by CODY Systems. Information is below.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Please direct questions to Laura Milford at lmilford@nfcausa.org or 858-602-6050.

Thank you for participating in the NFCA Sponsor Education Series.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series - May Calendar
Date: Saturday, May 8, 2021 4:24:41 PM
Attachments: May Calendar.pdf

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

The National Fusion Center Association (NFCA) announces the launch of its 2020 Sponsor Education Series. The Series is a monthly calendar of webinars presented by our valued NFCA sponsors to educate and inform the fusion center community about evolving technologies and services relevant to the fusion center mission.

Sessions are scheduled for Tuesday, Wednesday and Thursday afternoons at 1:00 pm EST for 30 or 60 minutes.

The Sponsor Education Series schedule with session descriptions for May is attached. Please take a look and calendar time to attend sessions of interest to you.

If you have questions or need assistance, please contact Laura Milford, NFCA's sponsor liaison, at lmilford@nfcausa.org or 858-602-6050.

Thank you for your participation.

From: NFCA President
To: L Milford
Subject: National Fusion Center Association Sponsor Education Series Today at 1:00 pm EST: CODY Systems
Date: Wednesday, May 12, 2021 9:17:14 AM
Attachments: May Calendar.pdf

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

Today's Sponsor Education Series presentation is hosted CODY Systems. Session information and a registration link are below. Also attached is the May Sponsor Education Series calendar.

COBRAnet: Fusion Center Platform for Real-Time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data fusion technology fuels fusion centers with a one-stop search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider.

Registration Link: https://codysystems.zoom.us/meeting/register/tJ0ucuCsqTgpE9Mf1MOPLrbYz361PrqdF5uB

Thank you for participating in the NFCA Sponsor Education Series.

From: Cara-Lin Graham
To: Justin Dutra; dmartin@tivertonpoliceri.com; jpepjonovich@quincyma.gov; Clement, Michael (POL); Paul Gauvin; walter_correia@warehampolice.com
Subject: RE: ALPR Access
Date: Friday, October 29, 2021 3:11:13 PM
Attachments: image001.png
Flock-Cranston-MOU-NESPIN-signed.pdf

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

Lt. Dutra,

Please see attached signed MOU from NESPIN. Thank you for allowing access.

Cara Graham, C.I.C.A.
Manager, Criminal Intelligence Services
New England State Police Information Network
124 Grove Street, Suite 105
Franklin, MA 02038
(508) 528-8200 x207
cgraham@nespin.riss.net

Any attached document(s) may be encrypted and requires a password which will be provided in a subsequent e-mail.

If NESPIN has helped you in a recent case please let us know. Your successes are our successes!

Disclaimer: Data in public records, commercially available data sources and the internet can contain errors and are generally not totally free from defect. Data from these sources should not be considered definitively accurate, and all data we provide to you should be independently verified before taking any action based on the results.

This e-mail and any files transmitted with it are the property of NESPIN, are confidential, and are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s), or otherwise have reason to believe that you have received this message in error, please notify the sender at 508-528-8200 and delete this message immediately from your computer. Any other use, retention, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited.

From: Justin Dutra <jdutra@cranstonpoliceri.com>

Sent: Friday, October 29, 2021 11:12 AM
To: dmartin@tivertonpoliceri.com; jpepjonovich@quincyma.gov; Cara-Lin Graham <cgraham@nespin.riss.net>; michael.clement@state.ma.us; pgauvin@frpd.org; walter_correia@warehampolice.com
Subject: ALPR Access

Good Morning,

In response to recent requests for access to Cranston Police ALPR network, I have prepared a MOU which has been attached to this email. Please read, sign, and return for immediate access.

Thank you.

Respectfully,

Lieutenant Justin T. Dutra
Special Projects Lieutenant
Cranston Police Department
Desk (401) 477-5035
Cell (401) [redacted]
Email: jdutra@cranstonpoliceri.com

From: Myslinski, Tara (DOT)
To: Osborne, Chester (DOT)
Cc: Fitzgerald, Thomas (POL); Fenton, Eileen (DOT)
Subject: RE: c. 90 updates for FAST
Date: Monday, March 1, 2021 3:50:28 PM
Attachments: 700 CMR 7 Redline.docx

Here are the redlined regulations. I did not add anything about the natural gas weight exception because I think it's sufficiently covered in the proposed statute, but I can if you prefer.

Please send us any/all thoughts on these regs and the legislative drafts and we will do everything we can to move them along.

Thank you!

Tara Myslinski
Senior Lead Counsel, Regulatory & Compliance
MassDOT
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
Mobile: 857-360-6810
Tara.myslinski@dot.state.ma.us

MassDOT and the MBTA are subject to MGL: Chpt.66, Sec.10 Public Records Law. Email sent or received by MassDOT and MBTA employees are subject to these laws. Unless otherwise exempted from the public records law, senders and receivers of MassDOT and MBTA email should presume that the email are subject to release upon request, and to state record retention requirements.

Confidentiality Notice | This communication (including any attachments) is only intended for the user of the individual, or entity, to which it is directed. It may contain information that is privileged, confidential and exempt from disclosure under applicable law, and should not be read, copied or otherwise used by any other person. If received in error: please notify the sender immediately and delete the e-mail, and any attachment(s), from your system, without copying, forwarding, disclosing or using it in any other way.

From: Myslinski, Tara (DOT)
Sent: Monday, March 1, 2021 2:05 PM
To: Osborne, Chester (DOT) <Chester.Osborne@dot.state.ma.us>
Cc: Fitzgerald, Thomas (POL) <thomas.fitzgerald@pol.state.ma.us>; Fenton, Eileen (DOT) <Eileen.Fenton@dot.state.ma.us>
Subject: c. 90 updates for FAST

Chester and Lieutenant:

Please see the attached suggested changes in c. 90 to conform to the FAST act. I hope this captures everything. From here, I'm going to go through our regs and make additional redlines – hoping to send you those today too.

Note that statutory amendments are difficult to accomplish and I can't predict their passage; regs are far easier. Because this is necessary to comply with federal requirements, however, perhaps we can fast track the legislation.

I am hoping you might be able to go through these in concept with FHWA tomorrow.

Tara

Tara Myslinski
Senior Lead Counsel, Regulatory & Compliance
MassDOT
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
Mobile: 857-360-6810
Tara.myslinski@dot.state.ma.us



MassDOT and the MBTA are subject to MGL: Chpt.66, Sec.10 Public Records Law. Email sent or received by MassDOT and MBTA employees are subject to these laws. Unless otherwise exempted from the public records law, senders and receivers of MassDOT and MBTA email should presume that the email are subject to release upon request, and to state record retention requirements.

Confidentiality Notice | This communication (including any attachments) is only intended for the user of the individual, or entity, to which it is directed. It may contain information that is privileged, confidential and exempt from disclosure under applicable law, and should not be read, copied or otherwise used by any other person. If received in error: please notify the sender immediately and delete the e-mail, and any attachment(s), from your system, without copying, forwarding, disclosing or using it in any other way.

From: Bender, Sean (POL)
To: Range, Scott (POL)
Subject: Re: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP
Date: Monday, April 5, 2021 12:00:03 PM
Attachments: HIDTA_NCRIC CONOP MAY2020.docx
Approved NCHIDTA NCRIC Policy Manual_19MAY2020 6.30.20 V2.docx

---

Certainly. Attached.

Respectfully,

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

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Monday, April 5, 2021 11:53 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

No rush, can you please see if you can un-pdf these?

Thanks

From: Range, Scott (POL)
Sent: Monday, March 8, 2021 2:59 PM
To: Gawron, Stephen (POL) <stephen.gawron@pol.state.ma.us>; Bandini, Brian (POL) (brian.bandini@pol.state.ma.us) <brian.bandini@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, March 8, 2021 2:53 PM
To: Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Monday, March 8, 2021 2:04 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Dermot,

Per your request…..lots (and lots) of info to digest here; however, I believe the most germane stuff you are looking for is contained in Sena's email below (as opposed to the enclosures).

Keep us posted. Talk soon.

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: Mike Sena [mailto:msena@ncric.ca.gov]
Sent: Sunday, March 7, 2021 2:58 PM
To: Fallon, Jay <jfallon@nehidta.org>
Subject: CJIS - Northern California HIDTA/NCRIC Policy, Procedure & CONOP

Jay,

Happy Sunday! We follow the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP) that also states that "All agencies applying for CLETS access must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP)".

We also require that all personnel, including contractors, must successfully complete a full law enforcement background. I've attached our Northern California HIDTA policy manual and concept of operations with the highlights below from the attached documents and the FBI CJIS Security Policy.

Please let me know if you need any additional information.

I'll talk with you soon.

Mike

Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020
https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Page i:

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

Page 7:

3.2.6 Contracting Government Agency (CGA) A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC) An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

2. Participate in related meetings and provide input and comments for system improvement.

3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with

permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.

9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

10. Any other responsibility for the AC promulgated by the FBI.

Northern CA HIDTA/NCRIC Policy & Procedure Manual Revised: May 2020

(Attached)

Beginning on page 80:

15.9.6 Use of Information

Under the provisions of California Penal Code section 502 et. seq., in addition to various federal codes, it is unlawful for any member of HIDTA/NCRIC to use information gained from any law enforcement and/or HIDTA/NCRIC databases for other than official business. Violations will be subject to disciplinary action and may be subject to criminal prosecution.

15.9.7 Criminal Data

The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). It is through this system that criminal history information is obtained through CLETS, as are all communications with other state, federal and international law enforcement agencies. The provisions of the CLETS User's Agreement govern the use of the CLETS system. All information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only. Access to this information is authorized only for personnel who have a legal right and need to know.

To maintain the integrity of the CLETS system and ensure the security of information

transmitted and received, all CLETS access equipment must be installed in compliance with the specifications in the CLETS User's Agreement. In addition to the CLETS User's Agreement, the use of CLETS is governed by California Penal Code Sections 182.1 and 502 (a) through (k), Vehicle Code Section 1808.21, 1808.47 and 1810.7.

The use of CLETS for other than authorized law enforcement may be prosecuted criminally under any of the above Code Sections. All members of HIDTA/NCRIC must use the CLETS system in compliance with the above agreements and laws.

15.9.8 Data Security

Data from the Department of Motor Vehicles (DMV) and Criminal History Information (CHI) on arrested persons are not public information. Under the provisions of California Penal Code sections 11075 through 11081, the Attorney General of California has established regulations governing the security and dissemination of such information (rap sheets). These regulations are specified in the CLETS User's Agreement. In compliance with these regulations, the following must be adhered to with regard to the processing of rap sheets.

Designated personnel serve as the Criminal Records Security Officer. The Criminal Records Security Officer is responsible for establishing and maintaining specific procedures for the handling of criminal history information and ensuring that every per-son with access to this information is fully trained in the procedures, regulations and laws promulgated by the State of California pertaining to the handling of this information.

Only designated managers, supervisors, intelligence officers, and analysts are authorized to release criminal history information. No other personnel shall release criminal history information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

15.9.9 Records Control

To ensure confidentiality of law enforcement records and criminal history reports, and to comply with the provisions of California Penal Code sections 11075 through 11081, the HIDTA/NCRIC CLETS Administrator will maintains a log that lists the CII number and the name of the subject of each report released to any authorized person. The audit log must include the date and time of the query, the name of the inquirer, the CII number of the target, the reason for the query (including a case number or name). CII information must be maintained in a manner consistent with the need to safeguard the material from unauthorized dissemination. When the record is no longer required, it must be purged.

15.10 Policy Conflict

The policies and procedures of the HIDTA/NCRIC are not intended to conflict with in-dividual agency guidelines or policies relative to information sharing, personnel and physical security, or other operational or administrative procedures. If a conflict does arise, the policies of the agency take precedence over these guidelines. A supervisor that is aware of a conflict shall notify the Executive director through the chain of com-mand as soon as possible.

15.10.1 DEA/ FBI /US DOJ/DHS/HIDTA/NCRIC Policy Conflict

HIDTA/NCRIC and ONDCP policies should not conflict with DEA, FBI/US DOJ and DHS policies and guidelines. If there is a conflict, the policies of DEA, FBI, US DOJ and DHS take precedence. In the event of a conflict, the executive director, or his/her designee, shall notify the appropriate SAC or the US Attorney of the conflict.

Northern CA HIDTA/NCRIC CONOP/Strategic Business Plan Revised: May 2020 (Attached)

Beginning on page 77:

Security

The HIDTA/NCRIC offices are in DEA, FBI, and task force-controlled facilities, rated to handle information up to the Secret classification level within the FBI and DEA facilities, and as such must comply with DEA and FBI security standards within those facilities. All HIDTA/NCRIC personnel are responsible to know and follow all adopted security guidelines and report violations of these guidelines to the appropriate FBI security officer, DEA security officer for the respective facility and the HIDTA/NCRIC security officer. The HIDTA/NCRIC Security Officer provide**s** regular security awareness training and serves as an available resource for HIDTA/NCRIC staff.

The HIDTA/NCRIC collects confidential and personal information from other agencies and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the California Attorney General's Criminal Intelligence File Guidelines, 28 Code of Federal Regulations (CFR) Part 23, Critical Infrastructure Information Act and the Information Sharing Environment's Functional Standards for Suspicious Activity Reporting. The HIDTA/NCRIC is committed to protect this information from unauthorized access, use, or disclosure. The following policies have been adopted to address employees' and/or contracted staff responsibilities for handling and protecting information

maintained in HIDTA/NCRIC data bases and files:

1. Employees and/or contracted staff assigned to the HIDTA/NCRIC, may access information only when necessary to perform work assigned by a supervisor to accomplish the HIDTA/NCRIC missions and objectives. HIDTA/NCRIC employees and contracted staff may not access or use information from the HIDTA/NCRIC data bases or from any other data base accessible through the CA DOJ/US DOJ/FBI/DEA/DHS data bases for personal reasons or any reason other than their duty assignment.

2. HIDTA/NCRIC staff may disclose confidential information from HIDTA/NCRIC files or data bases only to individuals who have been authorized to receive it through the appropriate procedures. HIDTA/NCRIC staff shall not divulge or make use of confidential information, data, or records of the HIDTA/NCRIC for a mailing list or any other purpose unless the same has been authorized. Such use is a misdemeanor under the California law.

3. HIDTA/NCRIC staff shall not deliberately enter false or incomplete data or delete existing valid data on any of the data bases or files. Staff shall not deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. As a precaution against misuse or destruction of information, HIDTA/NCRIC staff shall not remove any work-related materials from the work site without authorization to do so. Work in progress is to be stored and maintained in areas designated as appropriate for such storage and maintenance.

5. HIDTA/NCRIC staff shall take reasonable precautions to protect terminals and personal computers from unauthorized access. All HIDTA/NCRIC computers and portable devices shall always be protected by passphrase, password or biometric identification. Reasonable precautions include the following: ensuring that employee terminals are inaccessible when unattended; storing user documentation to sensitive programs in a secure place; and reporting any suspicious circumstances or unauthorized individuals observed in the work area to the employee's supervisor immediately.

From: Fallon, Jay <jfallon@nehidta.org>
Sent: Friday, March 5, 2021 7:12 AM
To: Mike Sena <msena@ncric.ca.gov>
Subject: Followup on MSP Brief

Mike,

As you are well aware, MSP brass was very favorably impressed with your knowledge and expertise relative to the ability to share info/intel with "contract" personnel, as opposed to "employees" and/or "sworn law enforcement". To that end, Colonel Quinn has requested any established policy/procedures you follow/have access to, specifically as it regards information/intelligence sharing access to CJIS data for/by contractor personnel.

Call should you need further clarification.

Thanks in advance. Greatly appreciate your efforts in this matter. J

Jay Fallon
Executive Director
New England HIDTA
978-691-2501

From: John Tedona
To: Pack, Noah (POL)
Subject: RE: Fixed & Mobile Locations
Date: Friday, December 10, 2021 11:53:39 AM
Attachments: image002.png
image003.png
image004.png
image007.png
image008.png
image009.png
Neology PAGIS-2.14 Software Training.pptx

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

The Audio file I sent you is the latest and only training material we have for BOSS. An update version will be available soon with additional function/feature descriptions and pop ups. Our BOSS Trainer can set up a webinar as needed for remote real-time training.

Regards,

John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Friday, December 10, 2021 11:19 AM
To: John Tedona <jtedona@neology.net>
Subject: Re: Fixed & Mobile Locations

Got it. Thanks John.

Do you have any other Boss 4 training materials that we can use - a PDF presentation or slide deck, for example? We need to plan how we are going to train our users and I imagine you have something we can use other than the video.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander

470 Worcester Road
Framingham, Massachusetts 01702

From: John Tedona <jtedona@neology.net>
Sent: Thursday, December 9, 2021 12:28 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Fixed & Mobile Locations

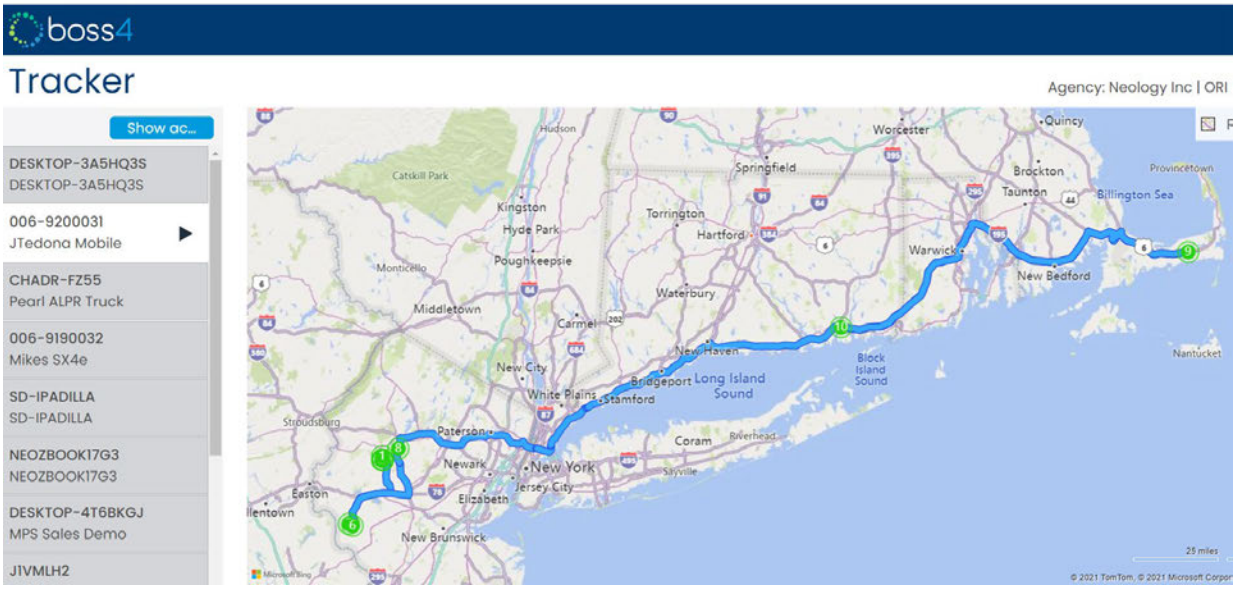
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Noah,

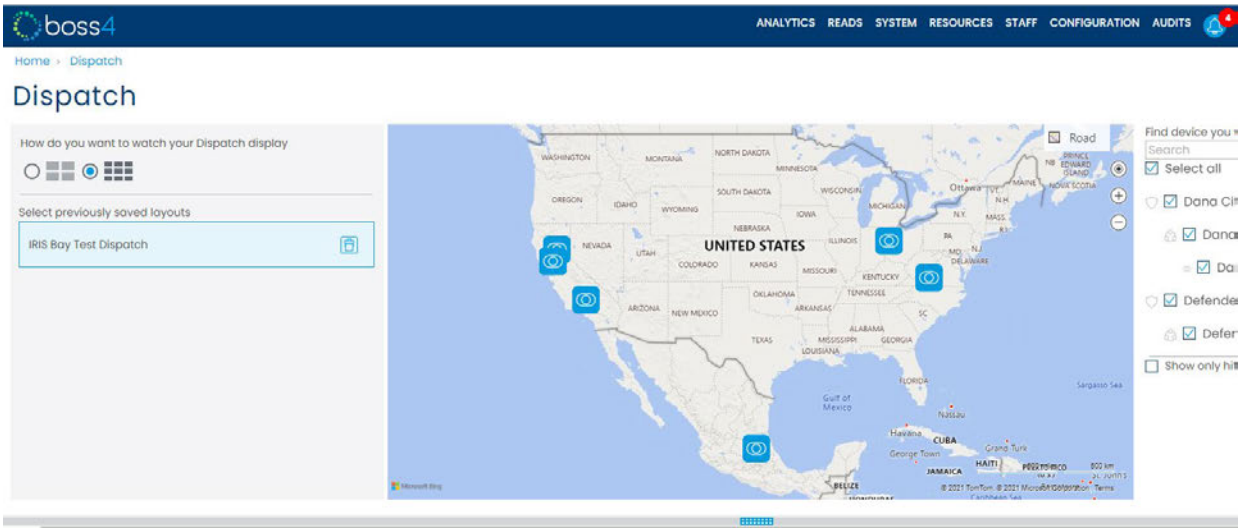
Circling back on your location question in BOSS. I listed a few BOSS screen shots that shows location information. View1 shows "Tracker" this can be turned on to show mobile locations in real-time or travel history, although I don't know of any agencies use this feature. This one shows my ALPR vehicle in some past travel.

View2 shows locations of Neology fixed demo cameras that are installed in the US. View3 shows a zoomed in view of one of the cameras in View2.

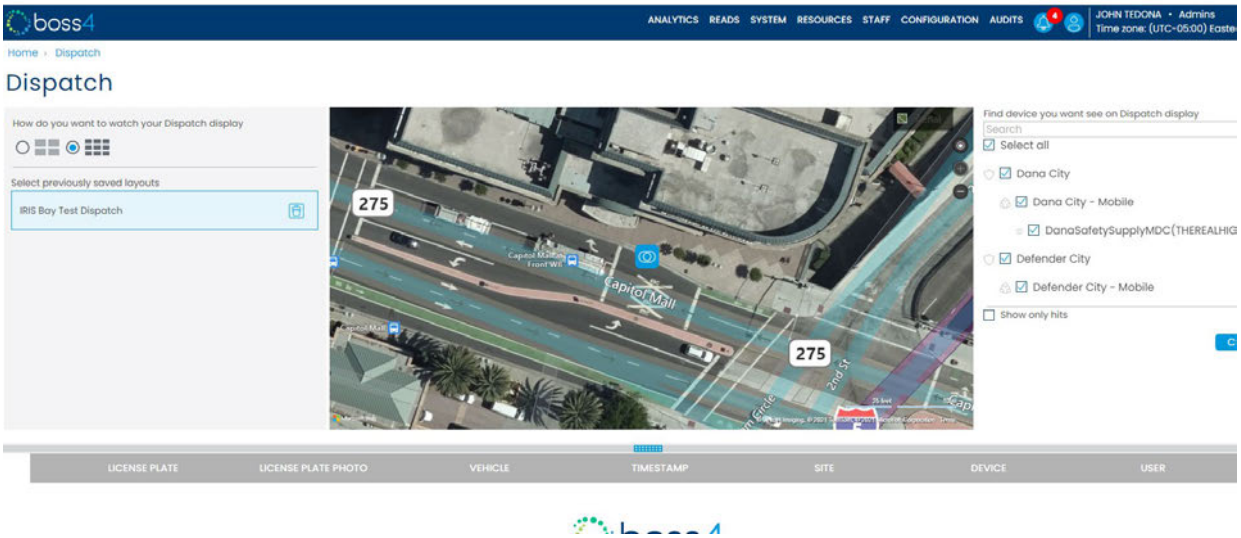
VIEW 1



VIEW 2



VIEW 3



John Tedona
Sales Manager

Mobile: 201-841-6237
Email: jtedona@neology.net

13520 Evening Creek Drive North, Suite 460
San Diego, CA 92128

www.neology.net

***Customer Support& Sales*:** (833) 747-7LPR or (833) 747-7577
Alpr_support@neology.net – Technical Service/Repair
Alpr@neology.net - Sales Inquiry

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

To: Wilcox, Christopher (POL)
Subject: RE: Genetic training
Date: Thursday, August 19, 2021 9:50:22 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

That sounds good, I recommend that TRF-11 be updated to reflect. Currently Field services owns it. I'll setup a meeting to begin a debrief.

-----Original Message-----
From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us>
Sent: Thursday, August 19, 2021 9:27 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Genetic training

Mark Cyr will oversee LPR Along with watch and fusion

LTC Chris Wilcox
Division of Homeland Security and Preparedness

> On Aug 19, 2021, at 9:21 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us> wrote:
>
> Yes
>
>> On Aug 19, 2021, at 9:12 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us> wrote:
>>
>> So is he coming up from Pennsylvania?
>>
>> LTC Chris Wilcox
>> Division of Homeland Security and Preparedness
>>
>>
>>>> On Aug 19, 2021, at 9:02 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>
>>> Just so you are aware this is a vistaCOM employee that would be onsite. BCM is the prime and passing through the cost.
>>>
>>>>> On Aug 19, 2021, at 7:56 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us> wrote:
>>>>
>>>> I forwarded this to Michelle we can talk about it next week
>>>>
>>>> LTC Chris Wilcox
>>>> Division of Homeland Security and Preparedness
>>>>
>>>>
>>>>>> On Aug 19, 2021, at 7:46 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>>>
>>>>> Do we want to adjust the time for the BCM tech?
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Tuesday, August 17, 2021 11:29 AM
>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>

>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Sounds good. Working on that stuff for you.
>>>>>
>>>>> For the AV technician on-site support we are looking at $4500. Are you good with that? If so I will send over a quote.
>>>>> It's not cheap, however it is a 4AM start on a holiday.
>>>>>
>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto
>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>
>>>>> On 8/17/21, 11:20 AM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> I'm looking for this
>>>>>
>>>>> SC-OTC-001 - Security Center - Omnicast Technical Certification
>>>>>
>>>>> And Maybe this
>>>>>
>>>>> SC-OTC-002 - Security Center - Omnicast Advanced Configuration and Troubleshooting
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Thursday, August 12, 2021 1:39 PM
>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>
>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Let me find out for you. What level of training are you interested in?
>>>>>
>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto

>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>> On 8/12/21, 1:35 PM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> What Genetec certificate courses do you guys provide or resell?
>>>>>
>>>>> Thanks
>>>>>
>>>>>
>>>>>

From: Egnitz, Brian (POL)
To: Wilcox, Christopher (POL)
Subject: RE: Genetic training
Date: Thursday, August 19, 2021 9:50:41 AM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

That sounds good, I recommend that TRF-11 be updated to reflect. Currently Field services owns it. I'll setup a meeting to begin a debrief.

Thanks, Brian

-----Original Message-----
From: Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us>
Sent: Thursday, August 19, 2021 9:27 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Genetic training

Mark Cyr will oversee LPR Along with watch and fusion

LTC Chris Wilcox
Division of Homeland Security and Preparedness

> On Aug 19, 2021, at 9:21 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us> wrote:
>
> Yes
>
>> On Aug 19, 2021, at 9:12 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us> wrote:
>>
>> So is he coming up from Pennsylvania?
>>
>> LTC Chris Wilcox
>> Division of Homeland Security and Preparedness
>>
>>
>>>> On Aug 19, 2021, at 9:02 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>
>>> Just so you are aware this is a vistaCOM employee that would be onsite. BCM is the prime and passing through the cost.
>>>
>>>>> On Aug 19, 2021, at 7:56 AM, Wilcox, Christopher (POL) <christopher.wilcox@pol.state ma.us> wrote:
>>>>
>>>> I forwarded this to Michelle we can talk about it next week
>>>>
>>>> LTC Chris Wilcox
>>>> Division of Homeland Security and Preparedness
>>>>
>>>>
>>>>>>> On Aug 19, 2021, at 7:46 AM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>>>
>>>>> Do we want to adjust the time for the BCM tech?
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Tuesday, August 17, 2021 11:29 AM

>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>
>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Sounds good. Working on that stuff for you.
>>>>>
>>>>> For the AV technician on-site support we are looking at $4500. Are you good with that? If so I will send over a quote.
>>>>> It's not cheap, however it is a 4AM start on a holiday.
>>>>>
>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto
>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>
>>>>> On 8/17/21, 11:20 AM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> I'm looking for this
>>>>>
>>>>> SC-OTC-001 - Security Center - Omnicast Technical Certification
>>>>>
>>>>> And Maybe this
>>>>>
>>>>> SC-OTC-002 - Security Center - Omnicast Advanced Configuration and Troubleshooting
>>>>>
>>>>> -----Original Message-----
>>>>> From: Boschetto, Matthew <Boschettom@bcmcontrols.com>
>>>>> Sent: Thursday, August 12, 2021 1:39 PM
>>>>> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>>> Subject: Re: Genetic training
>>>>>
>>>>>
>>>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>>>
>>>>>
>>>>> Brian,
>>>>>
>>>>> Let me find out for you. What level of training are you interested in?
>>>>>

>>>>> Cheers,
>>>>>
>>>>> Matthew Boschetto
>>>>> Account Manager | BCM Controls
>>>>> 30 Commerce Way, Woburn, MA 01801
>>>>> O: 781-897-5178
>>>>> C: 781-528-8344 | boschettom@bcmcontrols.com
>>>>>
>>>>>> On 8/12/21, 1:35 PM, "Egnitz, Brian (POL)" <brian.egnitz@state ma.us> wrote:
>>>>>
>>>>> WARNING: External Email
>>>>>
>>>>> _____
>>>>>
>>>>>
>>>>> Hi Matt,
>>>>>
>>>>> What Genetec certificate courses do you guys provide or resell?
>>>>>
>>>>> Thanks
>>>>>
>>>>>
>>>>>

From: Whittemore, Scott
To: Brooks, Brian (POL)
Subject: RE: policy draft
Date: Tuesday, April 6, 2021 2:32:47 PM
Attachments: LPR Policy.docx

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

Good Afternoon Sir-

I miss getting your requests for info on Holidays---

See attached. Let me know what else you need. This was based on the 'model' policy from DCJIS that was put out a few years ago.

Scott

From: Brooks, Brian (POL) <brian.brooks@state.ma.us>
Sent: Tuesday, April 6, 2021 2:12 PM
To: Whittemore, Scott <swhittemore@wellesleyma.gov>
Subject: policy draft

[**EXTERNAL EMAIL :** This message originated outside of the TOWN OF WELLESLEY mail system. **DO NOT CLICK** on **links** or open **attachments** unless you are sure the content is safe.]

Deputy, do you have a policy in Wellesley for Vigilant? I believe Major Range was going to reach out to you, but I figured I'd try to get a head of it whereas we will require one here. Brian

From: Katabazi, Lydia (FMCSA)

To: AK - Debbie Leonardo; Inga Johnson; Katherine Hensley; AK - Katie Smith; AL - David Baxley; AL - Jay Starling; AL - Sherry Helms; AL - Trishawn Bell; AR - Christy Earnhart; AZ - Diane Quintana; AZ - Gloria Paul; AZ - Steven Kalina; CA - Angela Marbray; CA - Coral Barber; CA - Marvin Hardley; CA - Suk Medeiros; CO - Abigail Lopez; CO - Dina Smith; CO - Jennifer Ketterman; CO - Jenny Adler; CO - Kirstie Nixon; CO - Michael Wolfinger; CO - Pamela Krupe; CO - Shanielle Rodriguez; CT - Iliana Rodriguez; CT - Kelly O"Connell; CT - Lori Druan; CT - Vanita Smith; DC - Darnell Fountain; elaine.speller dc.gov; DC - Michael Williams; DE - Mark Eastburn; DE - Robyn Bose; FL - Jay Levenstein; FL - Judy Cruce; FL - Robyn Wilson; GA - Brent Bennett; GA - Jared Hill; george.white ct.gov; IA - Alexander Jansen; IA - Angel Robinson; IA - Brenda Freshour-Johnston; IA - Debbie Leib; IA - Deborah Roeder; IA - Mary Guillaume; ID - Alberto Gonzalez; ID - Craig Roberts; ID - Jerri Hunter; ID - Reymundo Rodriguez; IL - Jason Copelin; IL - Michelle Blackley; IL - Scott Tucker; IN - Sandy Bowling; IN - Trish Smith; IRP Inc. - Robin Murphy; tadams irpinc.org; jeffrey.a.oberdank dos.nh.gov; jsteeger@mt.gov <MT State Partner>; KS - Deann Williams; KS - Dena McDaniel; KS - Donald Lee; KS - Rodney Allen; KY - Drew Clark; KY - Jennifer Walton ; KY - Lee Wigginton; KY - Mary Cook; KY - Robin Snook; KY - Stacey Schultz; KY - Tom McDaniel; LA - Andrea Chapman; LA - Brady Pupera; LA - Jeffrey Simmons; Lee.Nagano@hawaii.gov <HI DOT>; Rizzuto, Elizabeth (DOT); Sheehan, Erin (DOT); Daley, Gretchen (DOT); Rogers, Jessica (DOT); MA - Lawrence Lowery; Armstrong, Leslie (DOT); Parrott, Lynn (DOT); Duff, Melissa (DOT); Leblanc, Michelle (DOT); Cox, Stephanie M. (DOT); MD - Jan Hejl; MD - Kevin Gamble; MD - Latonya Montgomery; ME - April Goodwin; ME - Chelsea Chase; ME - Stephen Ashcroft; MI - Amy Havens; MI - Christopher Blundell; MI - Dawn VanAken; MI - Kimberly Hengesbach; MI - Michael Butcher; MI - Rayne Sherman; MN - Emma Corrie; MN - Erica Baraglia; MN - Natalie Wendell; MO - Aaron Hubbard; MO - Kelly Ray; MO - Michael Yoder; MO - Nathan Fontaine; MS - Danielle Hughes; MT - Eric Belford; MT - Jodee Alm; MT - Tom Winfield; NC - Cheryl Stanfield; NC - Dennis T. Smith; NC - J Council; NC - L Tinsley; NC - P Jacobs; NC - Portia Manley; ND - Dave Wolf; ND - Kyle Larson; NE - Beth Hartley; NE - Cathy Beedle; NH - Cindy Douglas; Marshall, Eric; NH - Scott Bryer; NJ - Christine Inglin; NJ - James Walker; NJ - Tykarra Barnwell; NM - Bernadette Gonzales; NM - Teresa Valdez; NV - Andrea Burnell; NV - John Neese; NV - Regina Ward; NV - Richard Wagner; NY - Andrew Deseve; NY - Bryan Solek; NY - Karen Jewett; NY - Karen Paradise; NY - Mary Withkowski; OH - Carolyn Evanston; OH - Devon Riggins; OK - Laura Osborne; OK - Nick Hensler; OK - Scott Greenawalt; OR - Angela Forrette; OR - Audrey Lawson; OR - Hannah Wilson; OR - Jonathan Reimer; OR - Laurie Hall; PA - Craig Johnson; PA - Michelle FIsher; PA - Nicholas Melnick; PA - Sombrata Bandyopadhyay; PA - Tammy Kohr; PA - Tanya Cooper; RI - Larissa Skeritte; lisa.fresolone dmv.ri.gov; SC - Amber Keane; SC - Cassidy Cade; SC - Deborah Smith; SC - Ernestine Aiken; SC - Mechelle Samuel; Larrimore, Nancy; SC - Wilma Allen; scott.haneberg hawaii.gov; SD - Chris Keil; SD - Darrin Gerry; SD - Dawn Sass; SD - Monica Weischedel; Susan.chang hawaii.gov; TN - Allison Raymer; TN - Amanda Kessler; TN - Beverly Bowman; TN - Dana Lee; TN - Danielle Baines; TN - Jennifer Lanfair; TN - Joetta Alderson; TN - Loretta Wheeler; TN - Mark Thomas; TN - Rachel Greer; TN - Romany Hanna; TN - Ryan Biggs; TN - Sisilia Liu; TN - Travis Plotzer; TN - Tymicia Willis; TX - Grady Meyer; TX - John Poole; TX - Tammy Russ; UT - John Moody; UT - Paula Vanikiotis; UT - Stephen Goodrich; VA - Florence Jett; VA - Pat Wimberly; VA - Patrick Harrison; VA - Shannon Hardy; VA - Yolanda Fleming; VT - Lori Stiles; VT - Mark Huntington; VT - Michael Smith; WA - Cathy Field; WA - Debbie Sanders; WA - George Price; WA - Kyle Strozyk; WA - LaVonne Fromm; WA - Sean McCoy; WA - Vanessa Simpson; WA - Wesley Marks; WI - Dustin Sweeney; WI - Ehren Bittorf; WI - Kathleen Hamilton; WI - Megan Powers; WI (JJKeller) - Kelly Gehrke; WV - Teresa Schott; WV - Zoe Bender; WY - Deborah Lopez; WY - Katherine Darrah; WY - Shannon DeGrazio; Jeremy Arnold; AZ - Jerry Haupt; CA - Denis Tam; Camsys - Brian Stewart; CAPS - Jeremy Pate; Celtic - Jeff Morgan; Celtic - Joe McCormick; Celtic - Kris Weaver; Celtic - Lynn Watson; Celtic - Manish Gohil; Celtic - Samir Nayak; bob.sardo ct.gov; DE - Geri Smith; DE - Kevin Needham; Punita.Choxi state.de.us; DriveWyze - Sara Steele; Explore - Jeff Pieschke; Explore - Nikki Benz; Explore - Scott Baker; Explore - Seth Ostrander; Explore - Tom Reynolds; FAST - Email; FAST - Julie Doney; FAST - Julie Doney; FAST - Mohamed Metwally; FL - Elvaro Jimenez; FL - Rufus Mayo; FL - Scott Tomaszewski; GA - Hugo Hall; GA - Rao Gorti; GA - Tracie Scott; ID - Neil Snyder; IIS - Brian Heath; IIS - Fred Ko; IIS - Werner Fraga; IL - Angie Williams; IL - Marinda Beccue; IL - Michael Stout; IL - Peter Neff; IL - Rod Smith; IN - Ranganath Kore; IN - Ravi Surapaneni; IN - Rongqiu Shen; IN - Uma Muttavarapu; IRD - Debbia Sarvas; IRD - Josh Zacharias; ISP - Tracs Support; Iteris - Aaron Jenkins; Iteris - CVO Support; Iteris - Delaine Adkins; Iteris - Inspections; Iteris - Jason Bowden; Iteris - Thad Hoffman; KY - Andrew Williams; KY - Donald Price; LA - Terri Ungerman; Legatus - Joanna Masny; Legatus - Mike Holloman; Legatus - William Curry; Kovac, James (DOT); Hanson, Michelle (ATLAS); MA - Sye Chanthaboun; MD - Madison Lumpkin; MD - Natalie Grasso; MD - Patrick Strauch; ME - Ann Lamore; MI - Dan Meengs; MI (Fast) - Luke Kledzik; MI (Fast) - Nathan Schmidt; MI (Fast) - Tom Yao; MN - Alex Gohar; MN - Jenny Cai; MN - Mike Baker; MN - Steve Mueller; MO - Doug Abbott; MS - Billy Saxton; MS - Hubert Crook; MS - Richard Smith; MS - Wyatt Sanford; NC - Bruce Boaz; NC - Mike Spears; ND - Scott Moran; NDSU - Brenda Lantz; NE - John Casteel; NLETS - Dustin Green; NLETS - Kate Silhol; NLETS - Kyle Darnell; Helpdesk Nlets; NM - Ojito Prevatt; NY - Ben Johnston; NY - Darcel Forde; NY - Joanne Catallo; NY - Lisa Clark; NY - Sri Nadella; OH - Alan Martin; OH - Candace Marzec; OH - Kate Hatfield; OH - RK Bogue; OH - Russ Dunn; OH (Leonardo) - Cisco Gonzalez; OH (Leonardo) - Matt Maxwell; OR - Chris Howell; OR - Michael Hartman; PA - Greg Gelnett; PA - Pam Molison; PrePass - Jan Skouby; SC - Darl Neiswonger; SC - IT Support; SecureWatch24 - Pat Fox; Seikosoft - Jordan Hayashi; SWRI - Darin Parish; SWRI - Tammy Duncan; TX-DPS - Richard Jackson; UT - Doug Stuart; VT - Chris Pitt; VT - Kelly Reagan; WA - Someshwar Busi-kumar; WI - CVIEW Support; WI - DMV Production Support; WI - MCR Unit; WY - AJ Myers; AL - Brent Mcelvaine; AL - Captain Jessie Peoples; AL - Lt. David Colston; AL - Mark Neilson; AL - Sgt. Michael Griffies; AR - Major Jay Thompson; Dan Williams; CA - Capt. Sean Duryee; CA - Lt. Nicholas Doko; CA - Sgt. Jaime Nunez; CO - Jeff Sewell; CO - Maj. Jon Barba; CO - Trish Aragon; CT - Corporal Greg Zeoli; CT - Lt. Christopher Smith; Donald Bridge; James Schaefer; Daniel.Parks state.de.us; FL - Keith Westphal; GA - Lt. Brent Moore; GA - Major Johnny Jones; scott.haneberg hawaii.gov; Susan.chang hawaii.gov; IA - Chief David Lorenzen; ID - Capt. Shawn Staley; IN - Donna Luley; IN - Kim Judge; IN - Major Jon Smithers; KS - Capt. Wes Ludolph; KS - Tom Catania; KY - Jennifer Walton; John Smoot; KY - Truesdell Tristan; LA - Capt. David Templeton; LA - Lt. Rueben.Auter; LA - Sgt. Kirk Thibodeaux; Fitzgerald, Thomas (POL); Jrotz sha.state.md.us; MD - Kevin Hickey; MD - Lt. John Griffin; James Wright; MI - Captain Michael Krumm; MI - Jack Johnson; MI - Lt. Charles Black; MN - Capt. Jonathan Olsen; MN - Lt. Arthur "Lee" Gear; matt.sokol state.mn.us; Kevin Kelley; MS - Chief Willie Huff; Greg Watson; MS - Major Roderick

	Goode; Ted Grimes; jsteeger@mt.gov <MT State Partner>; Karen.Ward ncdps.gov; NC - Kendell Jackson; NC - Lt. Terry Robinson; NC - Myra Beckers; NC - Sgt. Steve Kirby; NC - Tim Peterson; ND - Lt. Mike Roark; NE - Capt. Gerry Krolikowski; Daniel Doggett; NH - Sgt. William Burke; NJ - Sgt. Scott Dorrler; NM - Jessica Gibson; NM - Joseph Romero; NM - Todd Cullers; NV - Linda Allred; NV - Lt. Don Plowman; NY - Chris Scharl; NY - Jean-Paul Paraskevas; NY - Jill LaManna; NY - Jonathan NiCastro; NY - Justin Zimmerman; NY - Lt. Joseph Huber; NY - Marc Berger; NY - Suzanne Keiffer; OH - Bob Hartman; Brandon.Evans dps.ohio.gov; OH - Lt. A Reimer; Justin Gandy; PA - Brian M. Carpenter; PA - Chris Keffer; Doug Kemp; PA - Lt. Robert Krol; PA - Lt. Stephen Adamczyk; PA - Sgt. Michael Pavelko; RI - Corp. Mark Perotti; RI - Sgt. John Furtado; RI - Trp. John Gadrow; SC - Capt. John Price; SC - Colonel Leroy Taylor; SC - Major Dean Dill; SC - William David Findlay; john.broers state.sd.us; SD - Joel Peterson; TN - Capt. Brandon Douglas; TN - Lt. Allen England; troythompson flhsmv.gov; steven.rundell dps.texas.gov; TX - Major Chris Nordloh; csheppick utah.gov; ron.maxey vsp.virginia.gov; VA - First Sgt. Shawn Gobble; VA - Sgt. Robert Alessi; VT - Corporal Matt Nesto; WA - Capt. Trisena Sharff; WA - Donald Knoop; WI - Lt. Karl Mittelstadt; WV - Jessica Gordon; rbunner psc.state.wv.us; rblankenship psc.state.wv.us; WY - Christina Helsel; Dan Wyrick
Cc:	DeLorenzo, Joseph (FMCSA); Keane, Tom (FMCSA); Mahorney, Bill (FMCSA); Liberatore, Thomas (FMCSA); Kelly, Thomas (FMCSA); White, Camille (FMCSA); Byrne, Angie (Volpe); PRISMTechnicalSupport; Tepp, Jacob (FMCSA); Price, Bryan (FMCSA); FMCSA_MCFSPM; MCDA
Subject:	Re: PRISM Technical Announcement - ISS Target File
Date:	Monday, February 22, 2021 6:32:37 PM
Attachments:	PRISM Technical Announcement ISS Target File.pdf

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

Greetings PRISM Partners,

A supplemental PRISM Target File called the Inspection Selection System (ISS) Target File is currently available for State Law Enforcement to download and use to support roadside enforcement.

The ISS Target file is intended to provide additional information to State law enforcement to strategically and efficiently identify commercial motor vehicles for inspection by linking the motor carrier's ISS score to the vehicle registration record using the U.S. Department of Transportation (USDOT) number.

State Law Enforcement can utilize the ISS Target File with an Automated License Plate Reader (ALPR) to search and associate the ISS Score with the license plate at roadside to distinguish commercial motor vehicles that are linked to motor carriers with a higher safety risk.

The ISS Target File is used for Roadside enforcement only and is not a requirement to participate in PRISM.

Please see attached Announcement for details and let us know if you have any questions.

Thank you,

Lydia Katabazi

Lydia T. Katabazi
PRISM Program Manager
USDOT | FMCSA | Enforcement Division

1200 New Jersey Ave, SE, W63-455, Washington, DC 20590
☎Office: 202.366.0991 | ✉Email: Lydia.Katabazi@dot.gov

From: Peter Crary
To: Merrill, William R. (EOTSS)
Cc: Zhong, Henry; Chandler, Rob; Mitchell, Timothy P. (EOTSS); Velez, Mario; Dewey, Heather; Egnitz, Brian (POL); Osman, Ashraf; Novak, Marsel; Tom Cobb; Sullivan, Margaret (POL); Ramsay, Christopher B. (EOTSS); Stockwell, Matthew R. (EOTSS)
Subject: Re: Snowball - Neology+ Mass St Police
Date: Friday, September 17, 2021 4:30:24 PM
Attachments: image001.png

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

I sent it to Tim and Brian.

Peter Crary
Global R&D Director, ALPR
Neology, Inc
(Sent from my iPhone)

> On Sep 17, 2021, at 15:29, Merrill, William R (MASSIT) <william.r.merrill@state.ma.us> wrote:
>
> So on Step 4 I believe the confusion lies. Where does the unlock code come from and what is manifest? Is that the command to use in the command line interface?
>
> -bill
>
> **From:** Zhong, Henry <henzhong@amazon.com>
> **Sent:** Friday, September 17, 2021 4:25 PM
> **To:** Merrill, William R. (EOTSS) <William.R.Merrill@mass.gov>; Chandler, Rob <rbchand@amazon.com>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>; Velez, Mario <marvlez@amazon.com>; Dewey, Heather <hdewey@amazon.com>
> **Cc:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>; Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Ramsay, Christopher B. (EOTSS) <Christopher.B.Ramsay@mass.gov>; Stockwell, Matthew R. (EOTSS) <Matthew.R.Stockwell@mass.gov>
> **Subject:** Re: Snowball - Neology+ Mass St Police
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Bill

You are correct, the Snowball device and server with the snowball client will not need internet access. At high level you have the steps, I added step#4 authenticate the client to the snowball and #6 test run step .

1. Connect to switch via 10g copper
2. Configure static IP (no DHCP)
3. Install client on server
4. **Use manifest and unlock code to authenticate the Snowball client's access to a Snowball**
5. Initiate copy via command line
6. **Test run**
7. Profit

Henry Zhong | Solutions Architect, SLG Northeast
henzhong@amazon.com | Cell: [redacted]

From: "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>
Date: Friday, September 17, 2021 at 4:10 PM
To: "Zhong, Henry" <henzhong@amazon.com>, "Chandler, Rob" <rbchand@amazon.com>, "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>, "Velez, Mario" <marvlez@amazon.com>, "Dewey, Heather" <hdewey@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: RE: [EXTERNAL] Snowball - Neology+ Mass St Police

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

Hi Henry,

So to make it clear:

We already have the Snow device so the steps follow:

Connect to switch via 10g copper

Configure static IP (no DHCP)
Install client on server
Initiate copy via command line
??
??
Profit

At no point do we need to get the Snow device connected to the internet? Nor does the server with the client need to be connected to the internet? Sorry for all of the questions. We were looking to do a call but if my steps above are correct, we should be good to go.

-bill

From: Zhong, Henry <henzhong@amazon.com>
Sent: Friday, September 17, 2021 4:03 PM
To: Chandler, Rob <rbchand@amazon.com>; Merrill, William R. (EOTSS) <William.R.Merrill@mass.gov>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>; Velez, Mario <marvlez@amazon.com>; Dewey, Heather <hdewey@amazon.com>
Cc: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>; Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Ramsay, Christopher B. (EOTSS) <Christopher.B.Ramsay@mass.gov>; Stockwell, Matthew R. (EOTSS) <Matthew.R.Stockwell@mass.gov>
Subject: Re: Snowball - Neology+ Mass St Police

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

Hi Bill

The snowball client on the server and snowball device communication is encrypted in-transit; and during the request of snowball device in AWS console, an KMS(encryption key is added to encrypt data at rest.

Snowball device is configure to use DHCP and it will get an IP from your network DHCP server or you can change to static IP on the LCD display.

The server with data is on VM should not a problem; the team can run test to verify the

speed by copying files to another server.

Henry Zhong | Solutions Architect, SLG Northeast
henzhong@amazon.com | Cell: [redacted]

From: "Chandler, Rob" <rbchand@amazon.com>
Date: Friday, September 17, 2021 at 3:44 PM
To: "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>, "Zhong, Henry" <henzhong@amazon.com>, "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>, "Velez, Mario" <marvlez@amazon.com>, "Dewey, Heather" <hdewey@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: Re: [EXTERNAL] Snowball - Neology+ Mass St Police

I'm adding Heather and Mario from our Snow team to assist on these additional questions.

From: "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>
Date: Friday, September 17, 2021 at 12:42 PM
To: "Zhong, Henry" <henzhong@amazon.com>, "Chandler, Rob" <rbchand@amazon.com>, "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: RE: [EXTERNAL] Snowball - Neology+ Mass St Police

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

Thanks for the response Henry. One of the questions we had that were not completely clear in the documentation we reviewed was due to the encryption. Does the Snowball device need to be "enabled" before using via some hash? If we are going to plug it into a 10g copper switch, what other steps will we need to do? Assign it an IP? The server we are pulling the data from is a VM. Does that limit us somehow?

We will get the client/agent on the server in question and then start the copy process and that is that? When does the encryption of the data take place? During the transfer? At rest?

-bill

From: Zhong, Henry <henzhong@amazon.com>
Sent: Friday, September 17, 2021 3:24 PM
To: Chandler, Rob <rbchand@amazon.com>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>
Cc: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>; Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>; Ramsay, Christopher B. (EOTSS) <Christopher.B.Ramsay@mass.gov>; Merrill, William R. (EOTSS) <William.R.Merrill@mass.gov>; Stockwell, Matthew R. (EOTSS) <Matthew.R.Stockwell@mass.gov>
Subject: Re: Snowball - Neology+ Mass St Police

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

Hi Tim,

To copy 27TB of data to the snowball device will take some time depends on your local network speed between the server/snowball client and the snowball device. I include information outlines on how the network's transfer rate impacts how long it take to copy data to the device.
https://docs.aws.amazon.com/snowball/latest/ug/performance.html

To give some context here - if you are getting (~1 gig network) 100mb/second file copying speed from server to the snowball device on your network; then it will take about 3.12days to complete the 27TB of data. you can attempt multiple Snowball client workstations to improve performance/reduce time as suggested in the link above.

Snowball client workstation does not require internet access but you will need internet access to download the Snowball client from another workstation.
You can download the Snowball client from AWS Snowball resources.

Let us know if you have other question and happy to join a call with the team to walk thru the snowball client installations.

Thanks
Henry Zhong | Solutions Architect, SLG Northeast
henzhong@amazon.com | Cell: [redacted]

From: "Chandler, Rob" <rbchand@amazon.com>
Date: Friday, September 17, 2021 at 1:32 PM
To: "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>, "Zhong, Henry" <henzhong@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: Re: [EXTERNAL] Snowball - Neology+ Mass St Police

+Henry Zhong

From: "Mitchell, Timothy P (MASSIT)" <timothy.p.mitchell@state.ma.us>
Date: Friday, September 17, 2021 at 10:28 AM
To: "Chandler, Rob" <rbchand@amazon.com>
Cc: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>, Peter Crary <pcrary@neology.net>, "Osman, Ashraf" <ashrafo@elemental.com>, "Novak, Marsel" <marseln@amazon.com>, "Cobb, Tom" <cobthoma@amazon.com>, "Sullivan, Margaret (POL)" <margaret.sullivan@state.ma.us>, "Ramsay, Christopher B. (EOTSS)" <christopher.b.ramsay@state.ma.us>, "Merrill, William R (MASSIT)" <william.r.merrill@state.ma.us>, "Stockwell, Matthew R (MASSIT)" <matthew.r.stockwell@state.ma.us>
Subject: RE: [EXTERNAL] Snowball - Neology+ Mass St Police

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

Thank you for reaching out Rob.

I have copied the team from my side on this email. We are expecting to receive the Amazon Snowball device and need to figure out what we have to do to copy data from one 27T database to that device. In doing some preliminary reading about this we thought that the device needs network connectivity to the same subnet as the existing server to do the copying. Is that correct? Does the Snowball client need to be on a machine that has internet access as well as access to the snowball and database server in question? We have no prior experience with this and are looking for steps that we need to take to get this connected to the network/existing server.

Thank you

From: Chandler, Rob <rbchand@amazon.com>
Sent: Friday, September 17, 2021 12:37 PM
To: Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>
Cc: Peter Crary <pcrary@neology.net>; Osman, Ashraf <ashrafo@elemental.com>; Novak, Marsel <marseln@amazon.com>; Tom Cobb <cobthoma@amazon.com>
Subject: Snowball - Neology+ Mass St Police

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

Hi Tim,

I'm Neology's Account Manager here at AWS. Copying Tom and Marsel who support MSP. Ashraf is my technical counterpart.

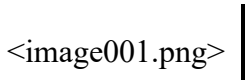
Peter let me know you had some questions regarding setting up Snowball and configuring the transfer.

Can you let us know what specific questions you have and hopefully we can resolve this quickly. If the account team can't resolve, we'll look at pulling in specialists as needed.

In case you haven't seen it, the docs are also quite extensive:
https://docs.aws.amazon.com/snowball/

Thanks,
Rob

_____



Rob Chandler
Account Manager - GovTech
Amazon Web Services
m: 410.212.3506

From: Pack, Noah (POL)
To: Wilcox, Christopher (POL)
Cc: Egnitz, Brian (POL)
Subject: Topics for Legal
Date: Tuesday, December 7, 2021 9:16:02 PM
Attachments: Flock Promo Description.pdf
MSP FLOCK MOU.pdf

Colonel:

The following topics are tentatively on our list to discuss at some point with legal:

1. MOUs:
    a. authorization/signatures for a usage MOU with Flock; MOU is attached
    b. when is an MOU is needed for other platforms?
    c. Flock data is free. Other platforms may be as well. Is there any issue with free LPR data from these companies?

2. LPR Infrastructure protection: discovery/FOIA
    a. For efficient management and deployment we'd like to create a map of LPR locations, but public release of same could result in widespread system damage/vandalism or avoidance
    b. How can we create but protect these documents?

3. Turnpike gantry LPR
    a. legal opinion of process required for investigative access per MGL
    b. developing a unified procedure & POC for exigent access

4. Use of new Boss4 LPR software purchased by Department:
    a. what should be on a splash screen (CJIS policy, anything else, requirement to agree in order to access)
    b. is splash screen sufficient to cover our members?

5. Tenant agencies contributing data:
    a. What do we require from them to accept their data?
        i. agency policy? any minimum standards? MOU?
        ii. we are awaiting some information from other agencies on what they do.
    b. Retention periods for locals policy may be less than 1 year.
        i. software setting appear to allow this, is it an issue to reduce retention period for some agency contributors?

6. Vigilant data:
    a. Department has purchased or obtained access to Vigilant national LPR database

through the Motorola body camera contract.

b. I'm working with DCapt. McCarthy for further info. There may be some questions on this related to commercial data, potential MOUs, etc. as we move forward. Inquiry for legal is incomplete at this point but should be resolved by time of meeting.

7. Flock nationwide study program:
    a. Through a partnership with Axon, Flock is offering a nationwide study/trial deployment that includes the free deployment of 25 cameras for one year, at locations of our choosing.
    b. They will handle deployment and cover the cost of all equipment and services for one year.
    c. They will make their SMEs and government affairs legal team available to us as needed.
    d. There is no obligation, and they will retrieve all devices and remove them after a year if we are not interested in an ongoing business relationship.
    e. This trial/study offer ends at the end of the calendar year, so we will need to make a decision shortly if we are able to do it.
    f. Preliminary info is attached.

8. Policy review and updates are pending in near future but not ready for discussion at this time.

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: 1 Ill. cop killed, 1 hurt in shooting; Watch: LEO lifts car off woman
Date: Wednesday, May 19, 2021 3:35:56 PM

May 19, 2021 | View as webpage

Dear Police1 Member,

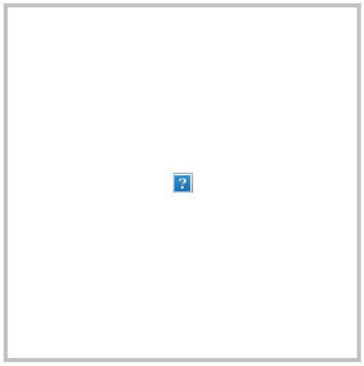
Ambushes seem to be happening with more frequency on traffic stops, disturbance calls and field contacts, to name just a few situations. Officers can increase their chances of survival by exercising good situational awareness and expecting the unexpected. Join us for a free webinar on May 26, sponsored by Leonardo, for a discussion of recent trends in ambush attacks and evolving prevention and response strategies.

Click here to reserve your spot.

Stay safe,

— The Police1 Team

TOP STORIES



Watch: Va. LEO single-handedly lifts car off trapped woman

Through "sheer will and determination" the deputy was able to physically lift the vehicle

Ill. police officer, suspect dead after exchange of gunfire

ND officer who suffered fatal medical emergency on duty ID'd

Push for Black applicants to take police test pays off, NYPD says

SC officer survives bullet in windshield as pursuit hits 100 mph

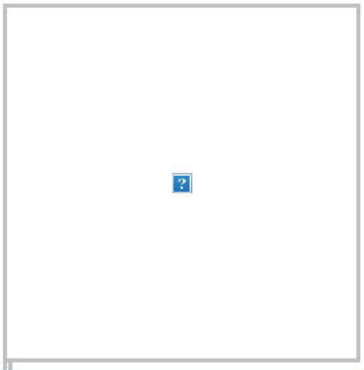
Wash. governor signs sweeping police reform measures

Protecting the Protectors



Southern Police Equipment – Shooters Kit with NIJ Level IV Plates

In stock now



#WELLNESSWEDNESDAY



Stinking thinking: How our thoughts determine how we feel

By Dr. Ellen Kirschman

When negative thoughts become habitual or are applied in the wrong context, they can be damaging



Enhancing first responder resilience through mindfulness

By Crawford Coates

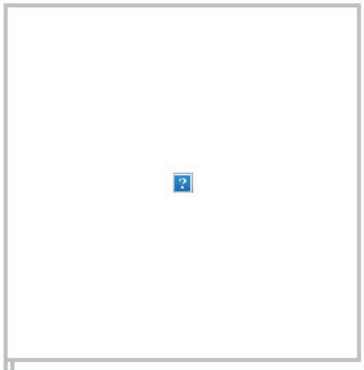
It's important to find a focused habit that energizes you and returns you to yourself as whole and complete



3 ways cops can take their physical performance to the next level

By Amir Khillah

Try the three moves described here by a fellow LEO to build strength and avoid injury



2020-2021 Ford Interceptor Utility VSX Console Series



Learn more about the ALL NEW VSX Console for Ford Interceptor Utility

Learn more

POLICE RESEARCH



Research: Detection of firearms by police officers and civilians

By Benjamin K. Barton, Ashley Bogar, and Casey Kovesdi

Researchers examined the ability of law enforcement officers and civilians to detect objects in the hands of other people



Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems



How collaborations with researchers can help LE agencies win grants

By Therese Matthews

In an era of evidence-based practices and smart policing, partnerships with academic institutions have bolstered police grant funding to support community safety



SPONSORED CONTENT



Start preparing for police camera

mandates
New bodycam and in-car camera requirements could cost your agency. Learn what most states will require, where to find grants and get tips on how to establish a program on May 27 at 2 p m. EDT.

FEATURED COMPANY NEWS

Digital Ally announces multiple law enforcement contracts awarded for body-worn and in-car camera systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Campus Safety Magazine
To: Grassia, Michael (POL)
Subject: 1 Student Killed, 1 Arrested in NM School Shooting
Date: Tuesday, August 17, 2021 10:01:45 AM

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

View on Web

CS Logo

August 17, 2021

1 Student Killed, 1 Arrested in New Mexico School Shooting

1 Student Killed, 1 Arrested in New Mexico School Shooting

The school shooting happened on the third day of classes and has prompted additional police presence on campus.

Fake COVID-19 Vaccination Cards a Concern for Colleges

A number of colleges are requiring students to show proof of vaccination, but are they ready to spot fakes and mete out appropriate discipline for violations?

CONTENT FROM OUR SPONSOR



Get Back to School Safely with ALPR

As students and staff get back to school, it is essential to make sure your campus is as safe as possible. Learn how Automatic License Plate Recognition (ALPR) technology can enable campus security and law enforcement to accurately monitor, predict and prevent crime on any type of campus.

Advertisement



Advertisement

Advertisement



Advertisement



Florida Public Schools Must Have Mobile Panic Alarms by 2021-22 Academic Year

The Martin County School District has installed an $800,000 Centegix alert system.



Auburn Issues Mobile Student IDs for Contactless Transactions and More

Auburn's mobile "Tiger Card" can be added to a student's iPhone, Apple Watch or Android Phone to open doors and pay for food and merchandise.



Designing a New Mass Notification System? Conduct a Risk Analysis

Identify your risks at the start of your mass notification project, but also during the project and for as long as the MNS system is in use.



St. Jude Pediatric Doctor: COVID Cases in Kids an 'Ominous Warning Sign'

As infection rates in children surge just as students go back to school, a St. Jude's pediatric doctor calls for increased action by all Americans to stop the delta variant.

Fortify your COVID-19 Mitigation Strategy with Real-time Monitoring on Campus

RESOURCE

Navigating the Return to In-Person School

Schools around the country are facing the dilemma of how to re-open schools while keeping students and staff safe. A number of technologies have emerged that can be useful in creating a COVID-safe environment but it can be challenging to identify which are the best fit for your school.

WEBCAST

The Latest Trends in Jeanne Clery Act Compliance

This session will provide tips on how to best deal with both the uncertainty and greater latitude introduced with the U.S. Department of Education's rescission of their compliance handbook last year.

Campus Safety Deep Dive: Access Control & Lockdown Special Report

Update My Preferences

©2021 Emerald X, LLC., All rights reserved.
31910 Del Obispo Suite 200 San Juan Capistrano, CA 92675

From: Campus Safety Magazine
To: Pirrotta, Melissa S. (POL)
Subject: 1 Student Killed, 1 Arrested in NM School Shooting
Date: Tuesday, August 17, 2021 10:02:44 AM

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

View on Web

CS Logo

August 17, 2021

1 Student Killed, 1 Arrested in New Mexico School Shooting

1 Student Killed, 1 Arrested in New Mexico School Shooting

The school shooting happened on the third day of classes and has prompted additional police presence on campus.

Fake COVID-19 Vaccination Cards a Concern for Colleges

A number of colleges are requiring students to show proof of vaccination, but are they ready to spot fakes and mete out appropriate discipline for violations?

CONTENT FROM OUR SPONSOR



Get Back to School Safely with ALPR

As students and staff get back to school, it is essential to make sure your campus is as safe as possible. Learn how Automatic License Plate Recognition (ALPR) technology can enable campus security and law enforcement to accurately monitor, predict and prevent crime on any type of campus.

Advertisement



Advertisement

Advertisement



Advertisement



Florida Public Schools Must Have Mobile Panic Alarms by 2021-22 Academic Year

The Martin County School District has installed an $800,000 Centegix alert system.



Auburn Issues Mobile Student IDs for Contactless Transactions and More

Auburn's mobile "Tiger Card" can be added to a student's iPhone, Apple Watch or Android Phone to open doors and pay for food and merchandise.



Designing a New Mass Notification System? Conduct a Risk Analysis

Identify your risks at the start of your mass notification project, but also during the project and for as long as the MNS system is in use.



St. Jude Pediatric Doctor: COVID Cases in Kids an 'Ominous Warning Sign'

As infection rates in children surge just as students go back to school, a St. Jude's pediatric doctor calls for increased action by all Americans to stop the delta variant.

Fortify your COVID-19 Mitigation Strategy with Real-time Monitoring on Campus

RESOURCE

Navigating the Return to In-Person School

Schools around the country are facing the dilemma of how to re-open schools while keeping students and staff safe. A number of technologies have emerged that can be useful in creating a COVID-safe environment but it can be challenging to identify which are the best fit for your school.

WEBCAST

The Latest Trends in Jeanne Clery Act Compliance

This session will provide tips on how to best deal with both the uncertainty and greater latitude introduced with the U.S. Department of Education's rescission of their compliance handbook last year.

Campus Safety Deep Dive: Access Control & Lockdown Special Report

Update My Preferences

©2021 Emerald X, LLC., All rights reserved.
31910 Del Obispo Suite 200 San Juan Capistrano, CA 92675

From:	McCarthy, Steven (POL)
To:	Amanda Regalado; Ethel Benhoff; Kevin Coughlin; Tiffany Morales; Jordan Carrick
Cc:	Mason, Christopher (POL); Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Collins, Kerry (EPS); Venkatachalam, Krishna (EPS); Robles, Francis Jr. (POL); Fernandes, Paul (POL); Liguori, MaryEllen (POL); Connor, Debora (POL); Mitchell, Timothy P. (EOTSS); deycleshymer@mhq.com; Ghasemi, Kiarash (EOTSS)
Subject:	APLR and 4RE decision
Date:	Wednesday, March 17, 2021 9:45:17 AM

Good morning,

As most of you all know, yesterday we completed the installation of ALPR on the fourth pilot vehicle. I greatly appreciate the assistance of EOTSS, Vigilant, and WatchGuard in equipping the vehicles so we could continue to test this feature on the 4RE. Unfortunately, the setup did not meet our expectations for performance.

Tuesday's test was conducted under virtually ideal conditions, bright filtered daylight, no fog/snow/or rain, with clean stationary license plates that were approached under a number of distances and camera angles, and the results mirrored the performance of last week's test. Capturing was spotty and unpredictable, some plates were read incorrectly, many were not read at all, and in most cases the states of the license plate were misreported.

This is no reflection on the WatchGuard 4RE, which appears to be an excellent vehicle video system. Nor does it undermine the Vigilant system, which also appears to be a powerful ALPR solution. What it does underscore is that the Vigilant system needs a purpose-built camera for robust APLR, and our general-purpose video camera is a poor fit to the system. The field of view for our Zero-sightline camera is simply too broad, and the lack of infrared capability on the camera further hampers the performance.

This feature was not an RFR requirement, and any optional stretch goal should never impair the mission critical purpose of the system, but frustratingly imperfect ALPR does indeed distract from the operations inside the cruiser. When viewed in the totality, the additional software footprint, the installation required, the complexity for the officer, coupled with disappointing performance, makes the decision about proceeding with this option a clear choice; we will not move forward with ALPR on the 4REs at this time.

The cost/benefit ratio simply is not there at this time. I have consulted with Colonel Mason and KP yesterday, and they agreed we should not try to implement something that will ultimately frustrate the officers.

Going forward we will forgo MHQ and EOTSS installing the ALPR cabling and software. The Department will continue to use the LEARN software for the trial year, this will consist of a few officers in Homeland Security who will be looking at its utility as the Department contemplates its future use of APLR. We will also remain open to considering its use in the future as the technology improves and new products are developed.

Thank you all for your efforts in trialing this feature. This is why we conduct pilots, to learn and make informed decisions, and in this case I believe this decision is the most appropriate one.

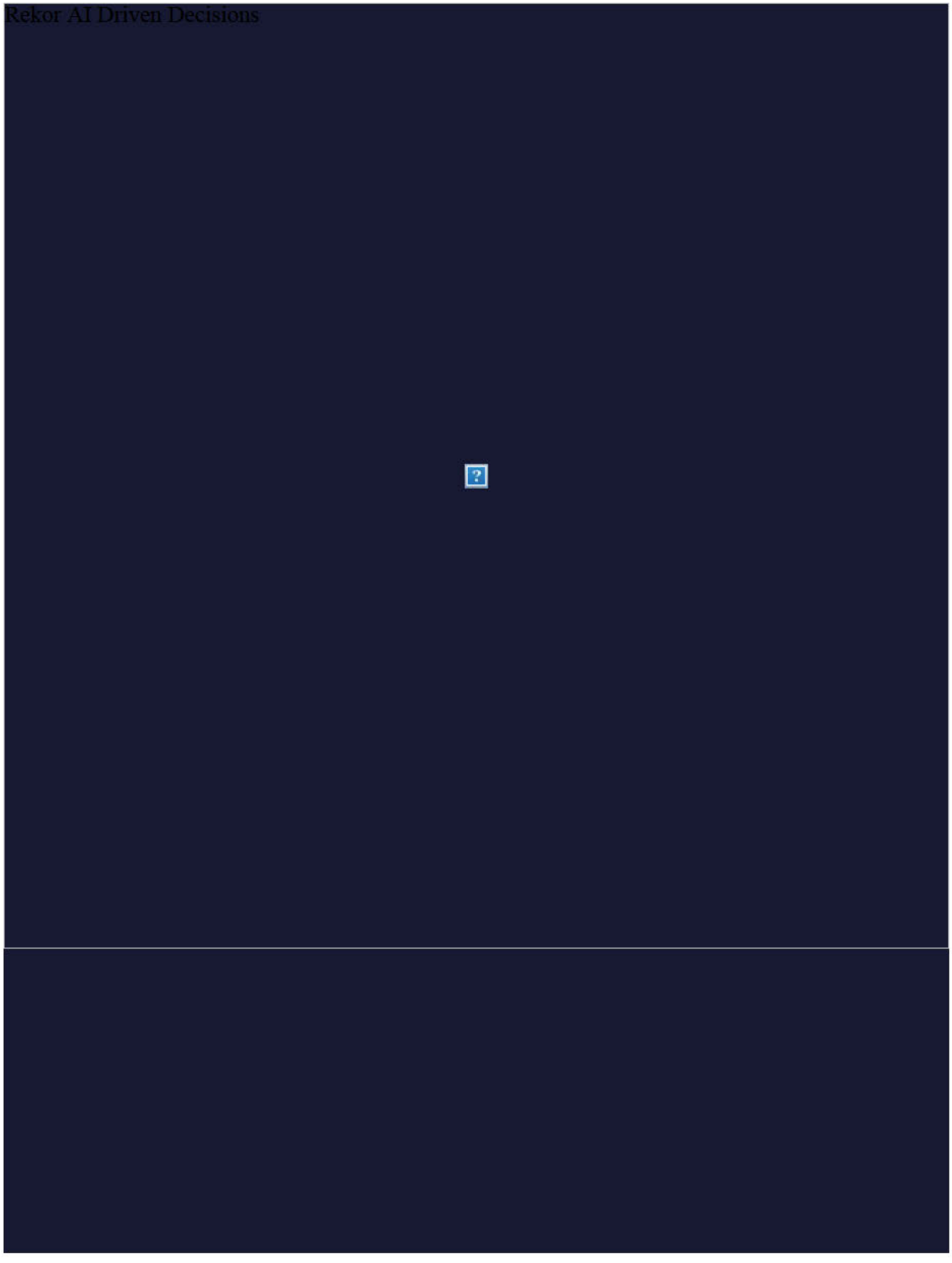
Respectfully,

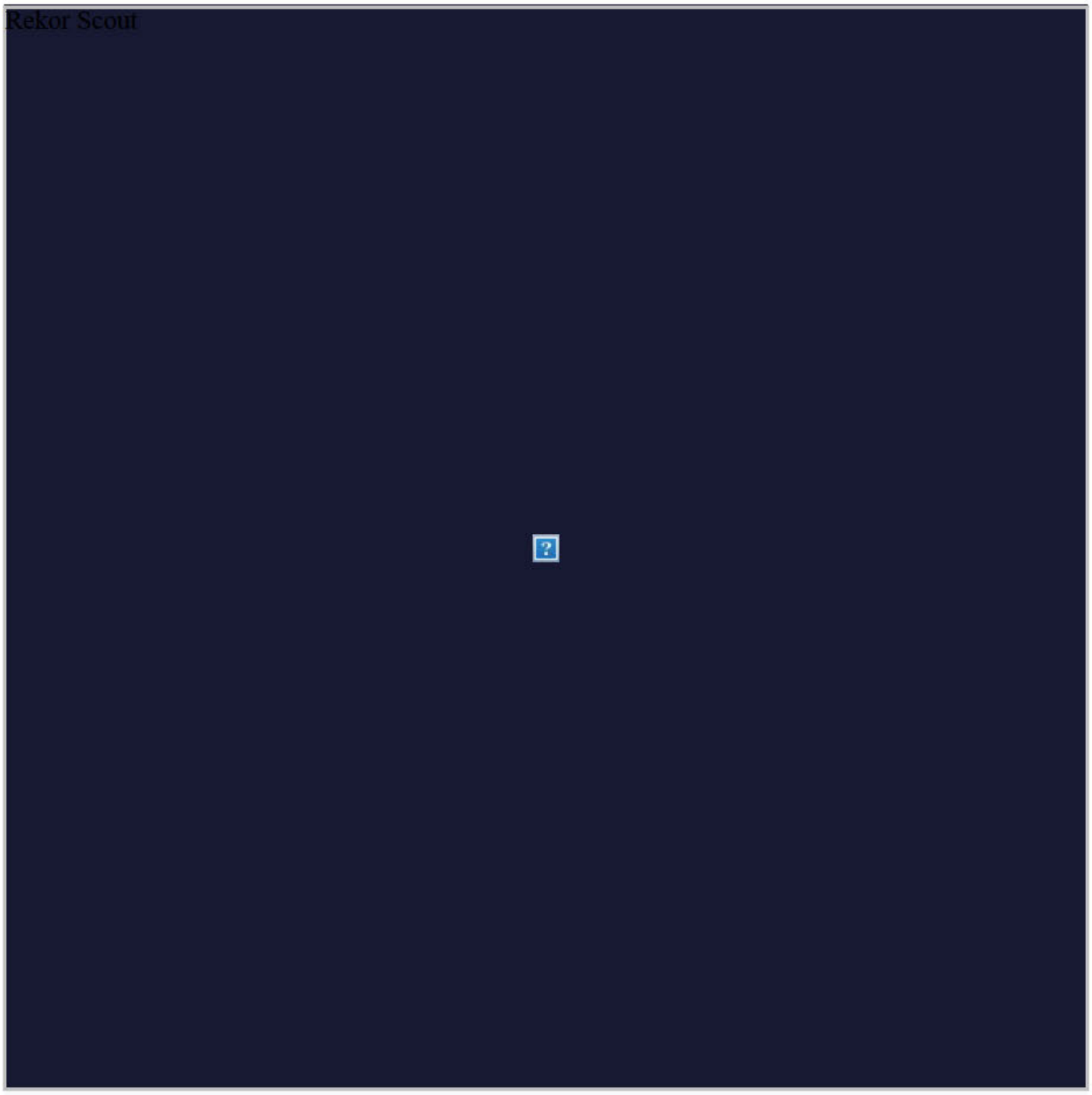
SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Police1 Product Alert
To: McCarthy, Steven (POL)
Subject: Are you looking for a way to prevent and solve crimes faster
Date: Thursday, April 22, 2021 10:45:13 AM

Having trouble viewing this email? View it in your browser.





Are you looking for a way to prevent and solve crimes faster?

Meet **Rekor**, leading provider in AI-Powered vehicle recognition solutions to federal, state, and local law enforcement agencies. Solutions specially designed for Law Enforcement ready to help you prevent and solve crimes.

Rekor Scout™ Benefits

FEATURED PRODUCT TO TAKE YOUR ALPR PROGRAM TO THE NEXT LEVEL:

Rekor Edge 300

Mountable Vehicle and License Plate Recognition System

- 3-4 lanes, 300 ft max range
- 120 mph max capture speed
- Surface or pole mountable
- Solar of direct power option

LEARN MORE



SEE MORE WITH REKOR

Ready to get started?

VIEW LAW ENFORCEMENT SOLUTIONS

Email us: sales@rekor.ai

Follow us:

Rekor Systems

7172 Columbia Gateway Dr. Su te 400 Columbia, MD 21046

www.rekor.ai • info@rekor.ai • 410.762.0800



If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Armed suspect steals cop car, is shot; SCOTUS expands meaning of "seizure"
Date: Friday, March 26, 2021 4:45:15 PM

March 26, 2021 | View as webpage

Dear Police1 Member,

The harsh reality of mental health services in the United States is that police are often the de facto first responders to people in crisis. Many law enforcement agencies have taken the laudable steps of staffing specialized response teams and training officers in crisis intervention. But tragic encounters between officers and people with mental health issues continue to occur.

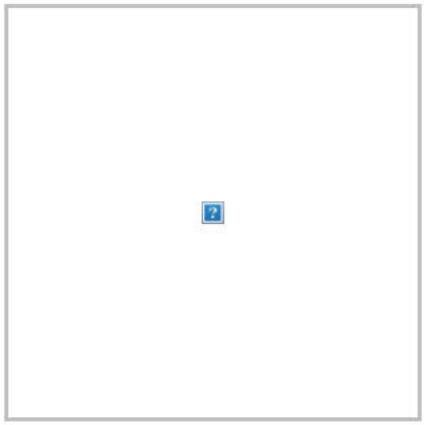
Lexipol's latest webinar on March 30 – Response to People in Crisis – will explore how crisis mitigation requires officers to draw on a different skillset than many other types of response. Attendees will learn tactics to de-escalate such situations and gain insight into the proper perspective to assist them when dealing with a person in crisis.

Register now and learn more about Lexipol's webinar series on police reform.

Stay safe,

— The Police1 Team

TOP STORIES



Police shoot, kill armed robbery suspect in stolen patrol car, ending standoff

The suspect led police on a pursuit that ended in a standoff with Massachusetts State Police

Ill. state trooper dies in car crash on duty

Supreme Court expands meaning of 'seizure' under 4th Amendment

Okla. deputy dies after altercation with jail detainee

NYC Council approves several sweeping police reform bills

Twin Cities 911 centers developing backup plans in preparation for Chauvin trial

Tactical Blanket Systems by Instant Armor



Lightweight, large coverage for officers against pistol and rifle fire. Find out why Instant Armor has been called the "most versatile piece of equipment" in the field.

Protect your officers

Low-cost Plate Reader for Agencies of All Sizes



Law enforcement agencies from small to large will save substantial amounts of time and money by automating license plate reading and processing with the low-cost ELSAG® VPH900 ALPR system.

Learn how

FEATURED CONTENT



This school resource officer and Olympic athlete has her sights on Tokyo

By Suzie Ziegler

It's not easy balancing Olympic dreams with being a cop, but Officer Jean says it's all about a strong mindset



Why code enforcement matters

By Policing Matters Podcast

Code enforcement officers play a key role in ensuring community safety while also facing significant safety risks themselves



Qualified immunity for LEOs is under assault: Will the doctrine survive the attack?

By Mike Callahan

If H.R. 1280 becomes law, the defense of qualified immunity for law enforcement officers will be abolished

How To Buy Online Training Systems



Download this Police1 buying guide to learn key steps for product selection, purchasing and implementation.

Download the free guide

Safe Fleet's Body-Worn Camera Solution



Some Focus X1 Body-Worn Camera advantages:
- High-Definition video resolution
- Rugged purpose built design for Law Enforcement
- Full-shift continuous recording and more

Visit Safe Fleet Law Enforcement

ARMORED RESCUE VEHICLES



Photo of the Week: BearCats mean

business

By Police1 Members

Armored vehicles manufacturer Lenco recently celebrated 40 years



Why cops need armored vehicles: 13 times BearCats saved lives

By Lt. Dan Marcou

Armored vehicles are not tanks – they are vehicles of refuge that serve to protect police and civilians alike



Training day: Armored vehicle breaching

By Lt. Matt Hardesty

Training to use an armored vehicle to breach a building is critical for successful deployment during tactical response



SPONSORED CONTENT



How to ensure clear tactical comms even with a mask

There's no room for miscommunication in a tactical situation. Here's how to wear a mask without sacrificing voice quality and clarity



FEATURED JOB



Alaska State Trooper Entry/Lateral ($10,000 Move Reimbursement)

Anchorage, AK

Entry Level: $34 98 hourly

FEATURED JOB



Seattle Police Dept. - Entry & Lateral Officers

Entry Level: $32.15 hourly



Pol ce1 does not send unsolic ted messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Vis t our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Craig Duncan
To: Foley, James (POL)
Subject: As a follow up to NIC, you"re invited to a HIDTA ALPR webinar
Date: Tuesday, September 28, 2021 8:32:54 AM

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

Leonardo

Hello Jay,

Thank you for taking the time to come by the Leonardo Inc./ELSAG ALPR Systems booth at the NIC Conference in Baltimore. As mentioned at the conference, we work closely with HIDTA and assist them in managing their Law Enforcement-only ALPR network. I will be sending out a meeting invite for a GoToMeeting webinar on the HIDTA ALPR Network that will be held on October 4th at 2:30 pm EST. Please feel free to forward the invite to anyone in your agency that may be interested.

About our collaborative relationship with HIDTA:
HIDTA is a data intrinsic organization committed to assist local LE agencies in their drug interdiction mission. The HIDTA ALPR Enterprise Operation Center(EOC) is a CJIS compliant data center server housed in the secure Houston Texas DEA HQ. It shares ALPR data interagency, allowing full access to investigators to query tags across the growing HIDTA ALPR network. EOC's push ALPR read data to the DEA DART/DICE server.

- HIDTA BOLO, DEA CAT4 hot list and multiple state and local level hot lists to be merged with NCIC list. Local agency 'private' hot lists can be set up and do not have to be shared.
- NO ONGOING USER LICENSES or USER FEES - ONE TIME EOC SYSTEM LICENSE
    - 2000+ ALPR cameras currently connected throughout the United States.
    - 1+ billion ALPR reads / 2.5 million LE ALPR reads per day inbound
    - 8,000 active LE users
    - 400+ active LE hot lists

Until then, please let me know if you have any questions.

Sincerely,
Craig Duncan
Sr. Field Operations Manager - Southeast
ELSAG ALPR Systems
Direct: +1 910-986-0596

PS. In the meantime, you may be interested in checking out **our LPR blog** for industry info and success stories.

Leonardo Company, 4221 Tudor Lane, Greensboro, North Carolina 27410
Unsubscribe Manage preferences

From: The Axon Team
To: McCarthy, Steven (POL)
Subject: Ask Rick Smith, CEO of Axon, anything...anything!
Date: Saturday, June 26, 2021 1:06:06 PM

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

Axon

Fleet 3 is hitting the road, and we want to know what you want to know.

Join Rick Smith, Chief Executive Officer, Jeff Kunins, Chief Product Officer, and Blake Bullock, Director of Fleet Products, for an Ask Me Anything-style webinar about our next-generation in-car camera system.

Curious about our integrated ALPR? Want to learn more about our Respond real-time alerts and streaming? Want to see how Fleet 3 can make your agency more efficient and collect better footage?

REGISTER NOW

We can't wait to hear from you!

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe





From: Axon Team
To: McCarthy, Thomas (POL)
Subject: Axon Release Notes and Updates for December 2021
Date: Tuesday, December 7, 2021 6:06:47 PM

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

Axon

THE LATEST AXON EVIDENCE RELEASE

Case Subfolders, Redaction Studio Updates, Auto-Transcribe download option updates, and more.

The December Axon release is coming soon. A high-level look at the changes is provided below, along with a link to the complete release notes with more details.

The December release is scheduled for December 14, 2021. Please refer to the Axon Evidence Maintenance Schedule on the Axon website for information on the updated schedule times for your region.

Take me to the release notes

What's New in Axon Evidence This Month:

- With the December release we are providing the ability to add **Case Subfolders**. This feature provides more flexibility when organizing evidence in a case and when importing evidence. **Note:** This feature is not enabled by default. If your agency would like to use this feature, contact your Axon representative.
- A **Redaction Studio** update that adds more blur level options in Redaction Studio and email notifications when Redaction Assistant completes redaction processing.
- We are adding more options when downloading transcriptions from **Auto-Transcribe** Transcription Assistant. These options allow users to customize the appearance of the downloaded transcript.
- Adding a new setting to the **TASER 7 and TASER 7 CQ setting pages**. The Cartridge

Deployment in Function Test Mode setting determines if the TASER 7 or TASER 7 CQ automatically exits Function Test Mode and deploys a cartridge when the trigger is pulled.

- On December 7 2021, we will begin deploying a new system for accessing your Axon accounts. This new **Sign In system** will resolve issues with our current Sign In experience and provide additional capabilities. This update will also include a new authenticator app for Multi-Factor Authentication.
- We are providing agencies the ability to have their **time format** changed from a 12-hour (AM/PM) format to a 24-hour time format. When enabled, all the times shown in Axon Evidence and the associated audit trails will use the 24-hour clock format. **Note:** This feature is not enabled by default. If your agency would like to use this feature, contact your Axon representative.
- To support the new **Axon Body 3 Wi-Fi Upload** feature, being released with Axon Body 3 camera Operating System (OS) v1.19, we are adding a new setting on the Axon Body 3 Camera Settings page and a new Body Camera Wi-Fi Networks page. The Automatic Wi-Fi Upload feature enables cameras to automatically upload evidence over Wi-Fi when in proximity to a pre-configured network. The Automatic Wi-Fi Upload feature is available for all Axon Body 3 customers and is not dependent on any unique licenses.
- When COVID-19 social-distancing measures and stay-at-home policies took effect in 2020 Axon announced we would make Citizen for Communities available for all agencies through the end of 2020. We extended this offering through 2021, but will be returning to the original licensing requirements starting in 2022. Contact your Axon representative for more information about plans and license requirements for **Axon Citizen**.
- Reminder, Axon has expanded **Email Notification Permissions** to provide agencies with more control on which users receive Axon operational emails, such as system service interruptions and release notes notifications.

Other Axon Product Updates:

- **Important Reminder**, at the end of December 2021 Axon will **end support for Internet Explorer 11 (IE11)**. See the full Release Notes for more information.
- The Axon Evidence Partner API has been updated to support performing external searches across your agency's ALPR records.
- In December, **Axon Performance** is making the new Command Hierarchy integration available to all customers. This integration leverages the Command Hierarchy functionality to make it easier to set up and maintain Groups in Axon Performance.
- In late December, we expect to begin deploying **Axon Body 3 camera** operating

system v1.19. This update will include the new Axon Body 3 Automatic Wi-Fi Upload feature, which provides the ability for cameras to automatically upload evidence throughout a user's shift using previously configured Wi-Fi networks.

- **Axon Interview** version 4.7.9 will be available in December. Axon Interview 4.7.9 includes general bug fixes and performance improvements for Livestreaming and Instant Playback.
- Starting in December, Axon will begin a phased deployment of firmware update bundle version 1.2143 for the **Axon Fleet 3 system**. The phased deployment will take approximately one month. See the full release notes for details on the update.
- A new iOS version of the **Axon Respond mobile app** will be released on December 7 2021. The new app has the same look and feature set as the previous version, and includes significant enhancements to performance and stability. It also introduces a fix for the sign in issue experienced by some Single Sign On (SSO) agencies.
- Axon is updating the supported operating system versions for our mobile applications. See the full release notes for details.

Coming Soon:

- Later this year we will be adding support **for playback of videos from ZIP files** in Axon Evidence. The new ZIP file support functionality will allow users to see the contents of a zipped file and create storyline presentations from videos in a ZIP file. This feature is currently in early access. Contact your Axon representative if your agency would like to participate in the early access.

As always, please refer to the **Complete Release Notes** for more information, including a list of resolved issues. The Axon Evidence Maintenance Schedule lists the updated schedule times for your region. We don't anticipate any downtime.

If you have any questions about the information in this release, please contact Technical Support.

North America: 1-800-978-2737 ext 4
UK: +44 1-327-709-666
Australia: 1-800-512-069
New Zealand: 1-800-005-161
International: See our Contact Us page
Email: support@axon.com

Sincerely,
The Axon Team

Axon Enterprise, Inc.

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe

From: Axon Team
To: McCarthy, Thomas (POL)
Subject: Axon Release Notes and Updates for October 2021
Date: Tuesday, October 19, 2021 6:09:01 PM

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

Axon

THE LATEST AXON EVIDENCE RELEASE

Command Hierarchy, Auto-Transcribe download options, Third-party video support update, and more.

The October Axon release is coming soon. A high-level look at the changes is provided below, along with a link to the complete release notes with more details.

The October release is scheduled for October 26, 2021. Please refer to the Axon Evidence Maintenance Schedule on the Axon website for information on the updated schedule times for your region.

Take me to the release notes

What's New in Axon Evidence This Month:

- With the October release we will deploy the **Command Hierarchy** feature, which allows agency administrators to model their agency's command structure with a hierarchical tree of command levels. This feature works in conjunction with the existing Groups functionality and users are added to groups to reflect their respective place in the command structure.
- We are adding new options when downloading transcriptions from **Auto-Transcribe** Transcription Assistant. These options allow users to customize the appearance of the downloaded transcript.
- When COVID-19 social-distancing measures and stay-at-home policies took effect in 2020 Axon announced we would make Citizen for Communities available for all agencies through the end of 2020. We extended this offering through 2021, but will

be returning to the original licensing requirements starting in 2022. Contact your Axon representative for more information about plans and license requirements for **Axon Citizen**.

- Axon Evidence is expanding the **Third-Party Video Support** functionality to include L3 .qbx files and .blk files.
- Reminder, Axon has expanded **Email Notification Permissions** to provide agencies with more control on which users receive Axon operational emails, such as system service interruptions and release notes notifications. We expect to implement the email notification change after the October release.

Other Axon Product Updates:

- The Axon Evidence Partner API has been updated to support getting GPS and time-series information from evidence files and ingesting ALPR hotlists.
- Starting in early November, Axon will begin a phased deployment of firmware update bundle v1.26 for the **Axon Fleet and Fleet 2 cameras**. The phased deployment will take approximately one month. See the full release notes for details on the update.
- The week of October 18, Axon will begin a phased release of **Axon Dock** firmware v3.14 with general bug fixes and performance improvements.
- **Axon Interview** version 4.7.7 will be available in late October. Axon Interview 4.7.7 includes general bug fixes and performance improvements. If you are using an older version of Axon Interview, we highly recommend upgrading to this version to take advantage of security updates released in version 4.7.
- Reminder, in December 2021 Axon will **end support for Internet Explorer 11 (IE11)**. See the full Release Notes for more information.
- **Upcoming Axon Release Schedule** - After October, there is only one more scheduled major releases for the 2021 calendar year: December 14, 2021. The November and December Axon Evidence releases are being combined into one release in order to avoid updates to Axon Evidence on the weeks of the US Thanksgiving holiday and year-end holidays in December.

Coming Soon:

- In December we expect to begin deploying **Axon Body 3 camera** operating system v1.19. This update will include the new Axon Body 3 Automatic Wi-Fi Upload feature, which provides the ability for cameras to automatically upload evidence throughout a user's shift using previously configured Wi-Fi networks.
- When the Command Hierarchy feature is deployed, we will launch the **Axon Performance - Command Hierarchy integration**. This integration leverages the Command Hierarchy functionality to make it easier to set up and maintain Groups in

Axon Performance. This integration is currently in early access. Contact your Axon representative if your agency would like to participate in the early access.

- Later this year we will be adding support **for playback of third-party videos from ZIP files** in Axon Evidence. The new ZIP file support functionality will allow users to see the contents of a zipped file and create storyline presentations from videos in a ZIP file. This feature is currently in early access. Contact your Axon representative if your agency would like to participate in the early access.
- In December 2021, we will be deploying a new system for accessing your Axon accounts. This new **Sign In system** will resolve issues with our current Sign In experience and provide additional capabilities. This update will also include a new authenticator app for Multi-Factor Authentication. We are opening this feature for early access in November. Contact your Axon representative if your agency would like to participate in the early access.

As always, please refer to the **Complete Release Notes** for more information, including a list of resolved issues. The Axon Evidence Maintenance Schedule lists the updated schedule times for your region. We don't anticipate any downtime.

If you have any questions about the information in this release, please contact Technical Support.

North America: 1-800-978-2737 ext 4
UK: +44 1-327-709-666
Australia: 1-800-512-069
New Zealand: 1-800-005-161
International: See our Contact Us page
Email: support@axon.com

Sincerely,
The Axon Team
Axon Enterprise, Inc.

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe





From: Axon Team
To: McCarthy, Thomas (POL)
Subject: Axon Release Notes and Updates for September 2021
Date: Tuesday, September 21, 2021 6:07:02 PM

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

Axon

THE LATEST AXON EVIDENCE RELEASE

Case Detail page filter updates, increased Session Timeout, and more.

The September Axon release is nearly here. A high-level look at the changes is provided below, along with a link to the complete release notes with more details.

The September release is scheduled for September 28, 2021. Please refer to the Axon Evidence Maintenance Schedule on the Axon website for information on the updated schedule times for your region.

Take me to the release notes

What's New in Axon Evidence This Month:

- Added the ability to **reset the search filters** on the Case Detail page - Evidence tab. This allows the user to quickly clear some or all the search filters being used when working with case evidence.
- The maximum value for the **Session Timeout** setting has been increased to 720 minutes. This change provides additional flexibility for agencies that need longer periods of inactivity before users are signed out.
- Reminder, Axon has expanded **Email Notification Permissions** to provide agencies with more control on which users receive Axon operational emails, such as system service interruptions and release notes notifications.

Other Axon Product Updates:

Axon Body 3 camera operating system v1.18 began a phased deployment in mid-September and is expected .to be available for all agencies the week of October 4, 2021.

- The Axon Evidence Partner API has been updated to support early access for the Command Hierarchy feature.
- Axon is introducing a new feature that allows Axon ALPR customers to selectively publish **ALPR policy and usage** information to a publicly available web page. This web page can then be linked to an agency's web page to facilitate transparency with the community and sustain community trust in the agency's ethical and compliant use of ALPR.
- Starting in early October, Axon will begin a phased deployment of firmware update bundle v1.2139 for the **Axon Fleet 3 system**. The phased deployment will take approximately one month. See the full release notes for details on the update.
- In late September, Axon will begin a phased release of **Axon View XL** v1.15.9 with updates for Standalone Mode and Fleet Mode. See the full release notes for details on the update.
- **Axon Interview** version 4.7 will be available at the end of September. This update adds the ability to add marker text without leaving the interview screen, adds a notification center to communicate important messages to Axon Interview administrators, and adds several security improvements.
- Reminder, in December 2021 Axon will **end support for Internet Explorer 11 (IE11)**. See the full Release Notes for more information.
- **Upcoming Axon Release Schedule** - After September, there are only two more scheduled major releases for the 2021 calendar year: October 26, 2021 and December 14, 2021. The November and December Axon Evidence releases are being combined into one release in order to avoid updates to Axon Evidence on the weeks of the US Thanksgiving holiday and year-end holidays in December.

Coming Soon:

- Later this year we will deploy the **Command Hierarchy** feature, which allows agency administrators to model their agency's command structure with a hierarchical tree of command levels. This feature works in conjunction with the existing Groups functionality and users are added to groups to reflect their respective place in the command structure. We are opening this feature for early access with the September release. Contact your Axon representative if your agency would like to participate in the early access.
- When the Command Hierarchy feature is deployed, we will launch the **Axon Performance - Command Hierarchy integration**. This integration leverages the

Command Hierarchy functionality to make it easier to set up and maintain Groups in Axon Performance. We are opening this integration for early access with the September release. Contact your Axon representative if your agency would like to participate in the early access.

- Later this year we will be adding support **for playback of third-party videos from ZIP files** in Axon Evidence. The new ZIP file support functionality will allow users to see the contents of a zipped file and create storyline presentations from videos in a ZIP file. We are opening this feature for early access with the September release. Contact your Axon representative if your agency would like to participate in the early access.
- In December 2021, we will be deploying a new system for accessing your Axon accounts. This new **Sign In system** will resolve issues with our current Sign In experience and provide additional capabilities. We are opening this feature for early access with the September release. Contact your Axon representative if your agency would like to participate in the early access.

As always, please refer to the **Complete Release Notes** for more information, including a list of resolved issues. The Axon Evidence Maintenance Schedule lists the updated schedule times for your region. We don't anticipate any downtime.

If you have any questions about the information in this release, please contact Technical Support.

North America: 1-800-978-2737 ext 4
UK: +44 1-327-709-666
Australia: 1-800-512-069
New Zealand: 1-800-005-161
International: See our Contact Us page
Email: support@axon.com

Sincerely,
The Axon Team
Axon Enterprise, Inc.

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe

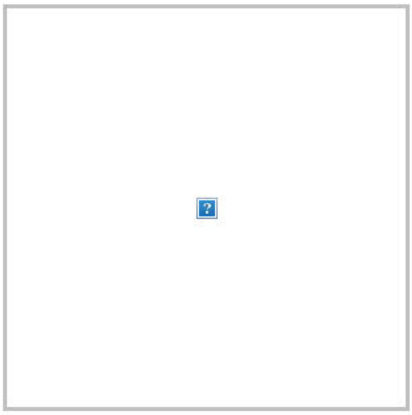




From: Police1 Roll Call
To: Clement, Michael (POL)
Subject: Bill letting cops sue protesters vetoed; Ban on PD"s thin blue line patches
Date: Thursday, August 12, 2021 3:10:49 PM

August 12, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



'I missed my job': Olympic hurdler returns to police work after Tokyo Games

When she's not chasing Olympic glory, Mulern Jean works as a school resource officer in South Carolina

NY bill that would have let police sue protesters is vetoed

Philly PD hit with contempt motions over not sharing misconduct data

San Diego-area police academy classes suspended over COVID cases

Ill. board votes to remove 'thin blue line' patches from police uniforms

Austin city leaders balk at $119M annual price tag of police ballot measure

Pair Your Wireless Earphones to your Radio



Air Pro Wireless Adapter lets you use your favorite earphones, like Apple Airpods, with your 2-way radio.

Shop adapters

Rekor Finder: Powerful & Discrete in-vehicle ALPR



Finder is a cost-effective, in-vehicle ALPR solution that accurately identifies license plates and vehicles in real-time at high speeds and extreme angles.

Learn more

FEATURED CONTENT



State your case: Should law enforcement agencies use unmarked vehicles for traffic enforcement?

By Jim Dudley and Chief Joel Shults, EdD

Despite fewer cars on the road due to COVID-related shutdowns, the national trend has been higher incidents of speeding and fatalities



Detention of man with AR-15 walking toward school was lawful

By Ken Wallen ine

The court noted that, given the mass murder at Marjory Stoneman Douglas High School, "any reasonable officer [would] be on heightened alert for copycat crimes"

Finally, Law Enforcement Technology for Everybody

Arrest to Adjudication: Agisent Technologies provides integrated solutions for agencies, prosecutors, and state-wide investigators: RMS ONE, PlatformRMS, ProDocs, ProCase, and Fusion Centers.

Grants, subsidies, and free-trials

Predict Criminal Patterns With ALPR

Learn how powerful ALPR cameras combined with advanced analysis software allow law enforcement to identify and predict suspect behaviors enabling them to effectively pursue and prevent crime.

Find out more

COLLEGE DEGREES IN LE

Opinion: Why the next generation of cops need a criminal justice degree

By Janay Gasparini, Ph.D.

Forging partnerships with faculty members at local colleges and universities can have a direct impact on the quality of officer candidates in your region

Why you should stop listening to the critics and go earn your college degree

By Marcus Rinaldi

A college education plays an important role in developing the interpersonal skills and

critical thinking required as a law enforcement officer

SPONSORED CONTENT

Does your department have a rugged, reliable and versatile drone?

A drone company known for its unique coaxial technology shares how it's changing the game for drone operations in public safety.

FEATURED RESOURCES

How to buy jail management software

Get the guide

FEATURED EDUCATION

Online M.S. in LE Leadership

Start your master's degree this year. Top-ranked program, 100% online.

FEATURED COMPANY NEWS

Estes AWS introduces 2021 Tahoe mounting solution

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Olivia Williams
To: Richard, Daniel (POL)
Subject: Calm Traffic & Capture License Plates Using one Mobile Unit
Date: Friday, December 3, 2021 1:23:12 PM

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

logo2.png

SpeedAlert radar message trailers equipped with automatic license plate recognition (ALPR) intelligence enable you to:

- **Effectively reduce speeding** in your community
- **Display drivers' speeds** along with custom speed-dependent messages
- **Capture license plates at high speeds** on streets and highways
- **Cover major city access points** for wanted vehicles
- **Collect traffic data** and efficiently resolve speeding complaints

Learn more about how SpeedAlert radar message trailers equipped with ALPR can help you keep your community safe.

"On a per-dollar basis, this might be one of the best expenditures we have."

– Councilmember Pasha Majdi, Vienna (VA) Town Council

All Traffic Solutions
14201 Sullyfield Circle Suite 300
Chantilly, VA 20151 USA
866.366.6602

You received this email because you are subscribed to Marketing Information from All Traffic Solutions.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails

From: Olivia Williams
To: Sonia, Michael (POL)
Subject: Calm Traffic & Capture License Plates Using one Mobile Unit
Date: Friday, December 3, 2021 1:22:48 PM

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

logo2.png

SpeedAlert radar message trailers equipped with automatic license plate recognition (ALPR) intelligence enable you to:

- **Effectively reduce speeding** in your community
- **Display drivers' speeds** along with custom speed-dependent messages
- **Capture license plates at high speeds** on streets and highways
- **Cover major city access points** for wanted vehicles
- **Collect traffic data** and efficiently resolve speeding complaints

Learn more about how SpeedAlert radar message trailers equipped with ALPR can help you keep your community safe.

"On a per-dollar basis, this might be one of the best expenditures we have."

– Councilmember Pasha Majdi, Vienna (VA) Town Council

All Traffic Solutions
14201 Sullyfield Circle Suite 300
Chantilly, VA 20151 USA
866.366.6602

You received this email because you are subscribed to Marketing Information from All Traffic Solutions.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails

From: Olivia Williams
To: Pollard, Peter (POL)
Subject: Calm Traffic & Capture License Plates Using one Mobile Unit
Date: Friday, December 3, 2021 1:22:45 PM

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

logo2.png

SpeedAlert radar message trailers equipped with automatic license plate recognition (ALPR) intelligence enable you to:

- **Effectively reduce speeding** in your community
- **Display drivers' speeds** along with custom speed-dependent messages
- **Capture license plates at high speeds** on streets and highways
- **Cover major city access points** for wanted vehicles
- **Collect traffic data** and efficiently resolve speeding complaints

Learn more about how SpeedAlert radar message trailers equipped with ALPR can help you keep your community safe.

"On a per-dollar basis, this might be one of the best expenditures we have."

– Councilmember Pasha Majdi, Vienna (VA) Town Council

All Traffic Solutions
14201 Sullyfield Circle Suite 300
Chantilly, VA 20151 USA
866.366.6602

You received this email because you are subscribed to Marketing Information from All Traffic Solutions.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails

From: Olivia Williams
To: Eng, Brian (POL)
Subject: Calm Traffic & Capture License Plates Using one Mobile Unit
Date: Friday, December 3, 2021 1:21:58 PM

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

logo2.png

SpeedAlert radar message trailers equipped with automatic license plate recognition (ALPR) intelligence enable you to:

- **Effectively reduce speeding** in your community
- **Display drivers' speeds** along with custom speed-dependent messages
- **Capture license plates at high speeds** on streets and highways
- **Cover major city access points** for wanted vehicles
- **Collect traffic data** and efficiently resolve speeding complaints

Learn more about how SpeedAlert radar message trailers equipped with ALPR can help you keep your community safe.

"On a per-dollar basis, this might be one of the best expenditures we have."

– Councilmember Pasha Majdi, Vienna (VA) Town Council

All Traffic Solutions
14201 Sullyfield Circle Suite 300
Chantilly, VA 20151 USA
866.366.6602

You received this email because you are subscribed to Marketing Information from All Traffic Solutions.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails

From: Olivia Williams
To: DeLong, Tyson (POL)
Subject: Calm Traffic & Capture License Plates Using one Mobile Unit
Date: Friday, December 3, 2021 1:20:50 PM

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

logo2.png

SpeedAlert radar message trailers equipped with automatic license plate recognition (ALPR) intelligence enable you to:

- **Effectively reduce speeding** in your community
- **Display drivers' speeds** along with custom speed-dependent messages
- **Capture license plates at high speeds** on streets and highways
- **Cover major city access points** for wanted vehicles
- **Collect traffic data** and efficiently resolve speeding complaints

Learn more about how SpeedAlert radar message trailers equipped with ALPR can help you keep your community safe.

"On a per-dollar basis, this might be one of the best expenditures we have."

– Councilmember Pasha Majdi, Vienna (VA) Town Council

All Traffic Solutions
14201 Sullyfield Circle Suite 300
Chantilly, VA 20151 USA
866.366.6602

You received this email because you are subscribed to Marketing Information from All Traffic Solutions.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails

From: Olivia Williams
To: Hathaway, David (POL)
Subject: Calm Traffic & Capture License Plates Using one Mobile Unit
Date: Friday, December 3, 2021 1:24:04 PM

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

logo2.png

SpeedAlert radar message trailers equipped with automatic license plate recognition (ALPR) intelligence enable you to:

- **Effectively reduce speeding** in your community
- **Display drivers' speeds** along with custom speed-dependent messages
- **Capture license plates at high speeds** on streets and highways
- **Cover major city access points** for wanted vehicles
- **Collect traffic data** and efficiently resolve speeding complaints

Learn more about how SpeedAlert radar message trailers equipped with ALPR can help you keep your community safe.

"On a per-dollar basis, this might be one of the best expenditures we have."

– Councilmember Pasha Majdi, Vienna (VA) Town Council

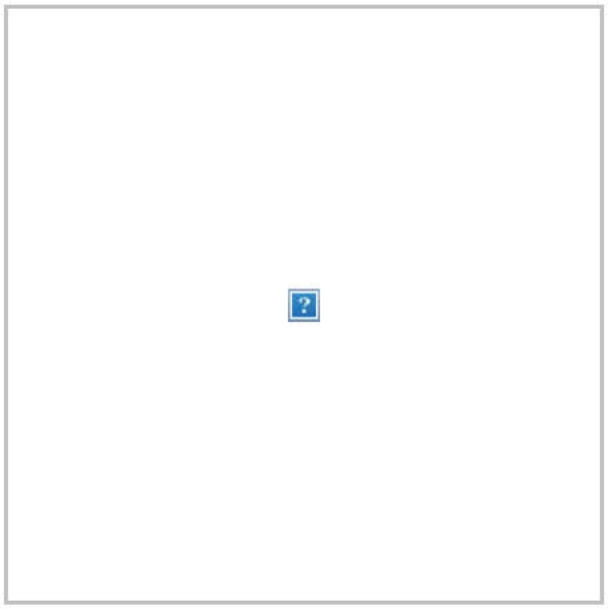
All Traffic Solutions
14201 Sullyfield Circle Suite 300
Chantilly, VA 20151 USA
866.366.6602

You received this email because you are subscribed to Marketing Information from All Traffic Solutions.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails

From: Police1 Product Alert
To: McCarthy, Steven (POL)
Subject: Catch more criminals using vehicle recognition technology
Date: Monday, April 12, 2021 5:35:19 PM

April 8, 2021 | View as webpage

SPONSORED BY



How to catch more criminals with a modular vehicle recognition system

Rekor Scout vehicle recognition software searches images for make, model, color and other distinct features associated with a stolen/wanted vehicle and provides automatic alerts when a match is found.

FEATURED CONTENT



How ALPR is scaring criminals away from this Tennessee town

Faced with a surge of out-of-town thieves, Mt. Juliet PD adopted an automatic license plate and vehicle recognition solution, resulting in more suspects caught and fewer crimes committed.



How AI and machine learning

drive more accurate vehicle recognition

A vehicle recognition system powered by artificial intelligence can help police catch more criminals by analyzing video in the background and providing alerts in real time.

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Grassia, Michael (POL)
Subject: Chicago mayor takes police union head to court over vax mandate
Date: Friday, October 15, 2021 3:12:50 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do

Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!

Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how

Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Tulipano, Michael (POL)
Subject: Chicago mayor takes police union head to court over vax mandate
Date: Friday, October 15, 2021 3:12:01 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

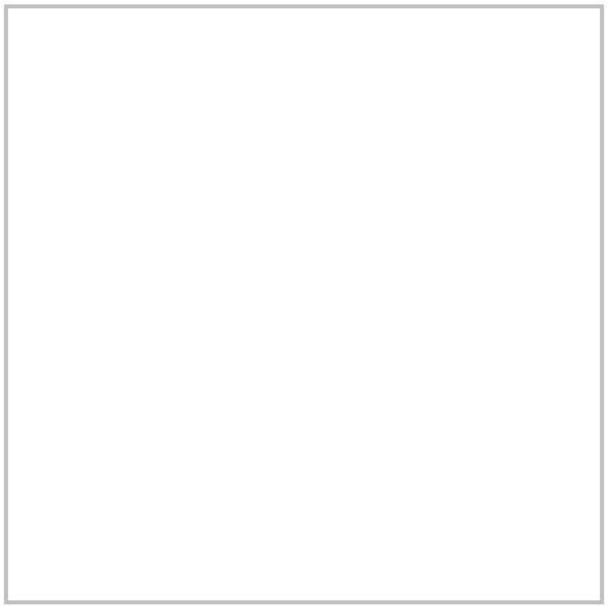
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

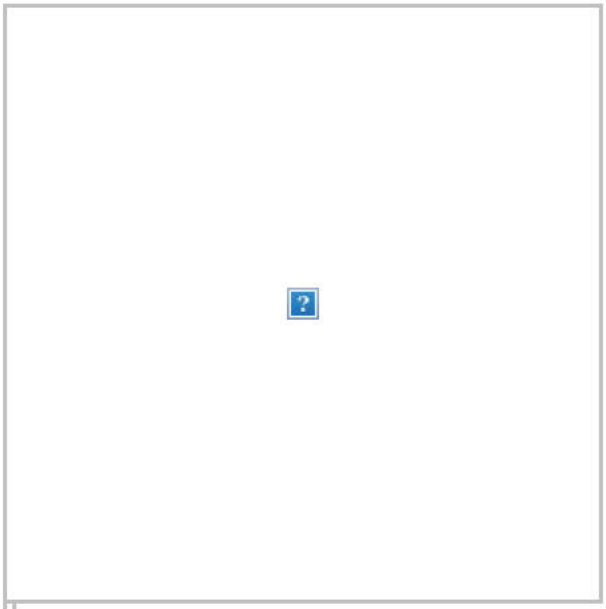
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



FEATURED CONTENT

Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Breton, Benjamin (POL)
Subject: Chicago mayor takes police union head to court over vax mandate
Date: Friday, October 15, 2021 3:12:27 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

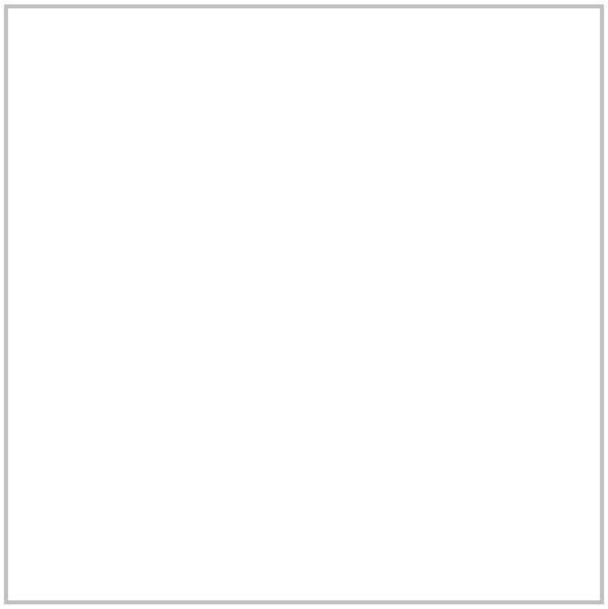
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

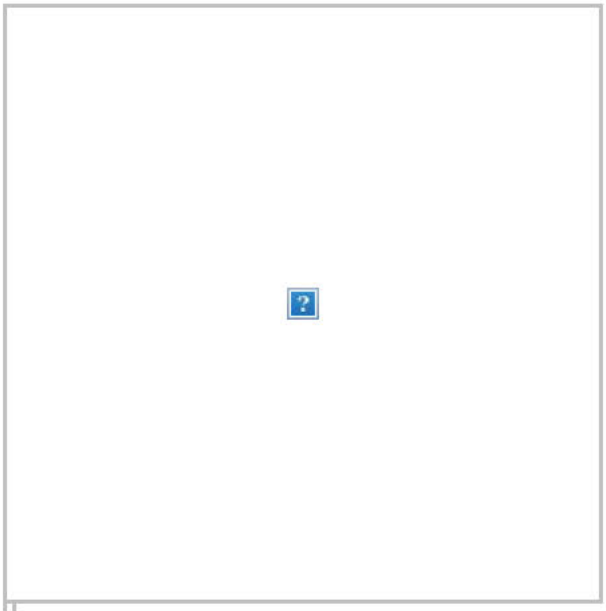
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Goonan, Michael D (POL)
Subject: Chicago mayor takes police union head to court over vax mandate
Date: Friday, October 15, 2021 3:12:12 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

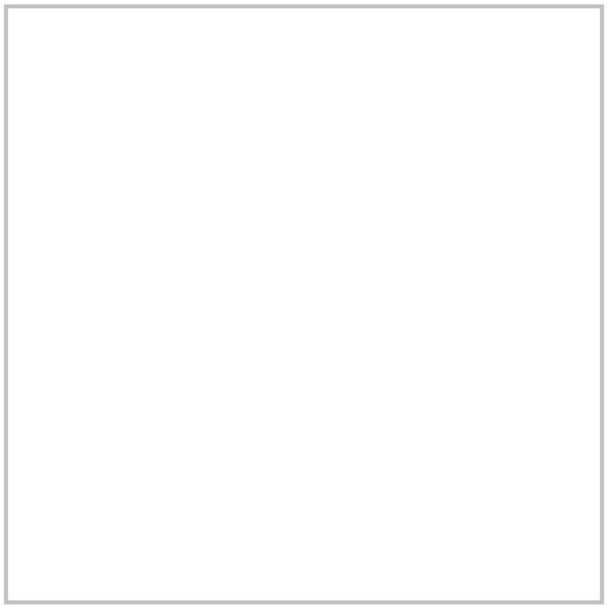
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

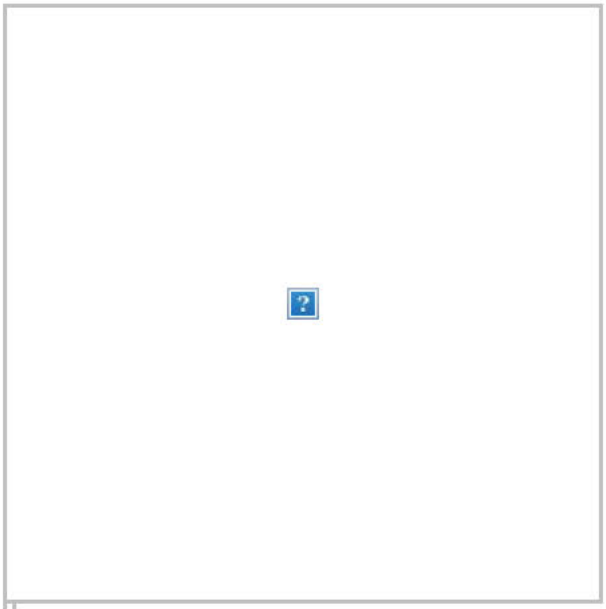
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



FEATURED CONTENT

Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Keville, Robert (POL)
Subject: Chicago mayor takes police union head to court over vax mandate
Date: Friday, October 15, 2021 3:11:09 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

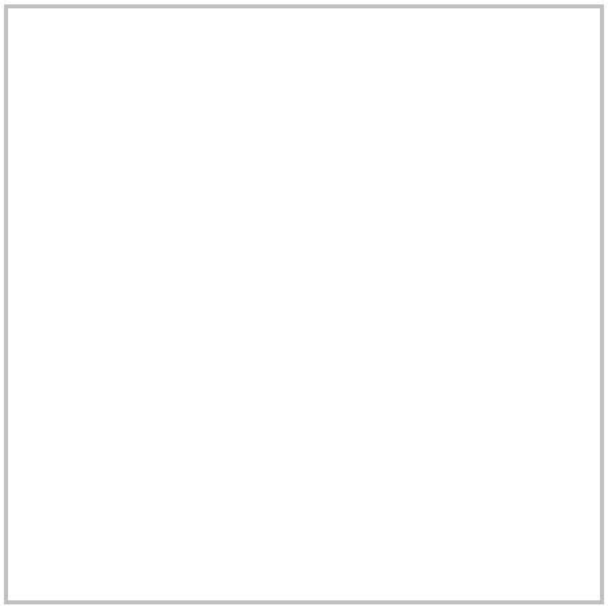
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

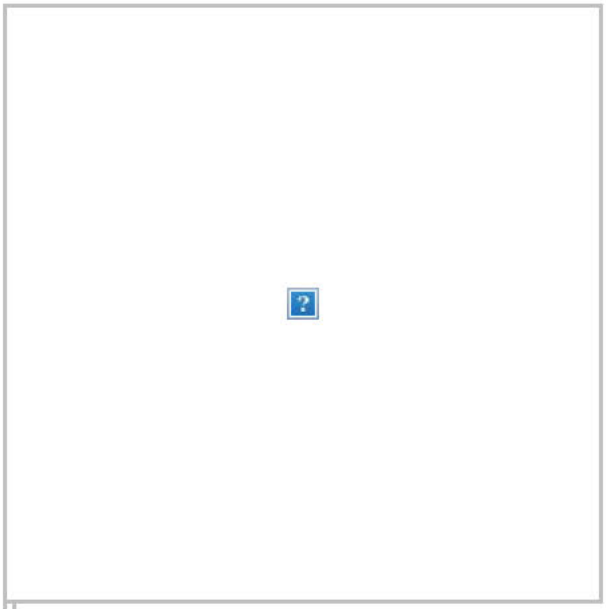
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: benesh, meghann E (POL)
Subject: Chicago mayor takes police union head to court over vax mandate
Date: Friday, October 15, 2021 3:14:52 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

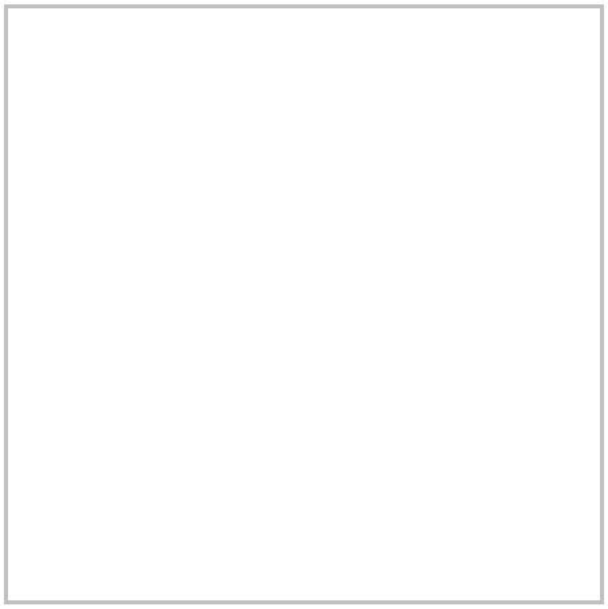
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

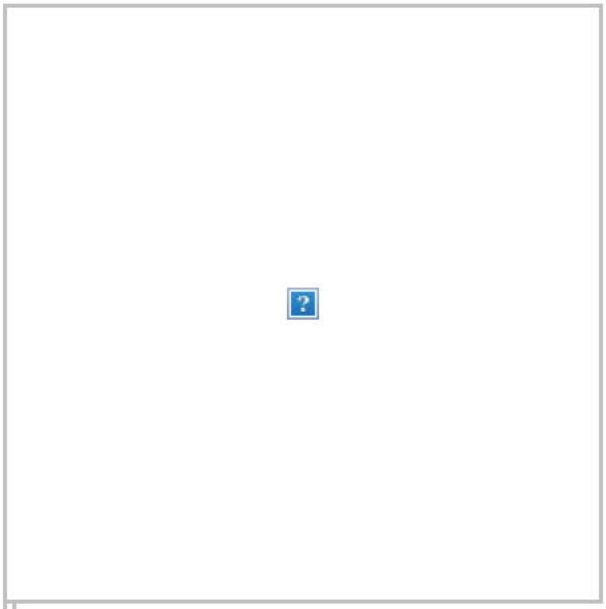
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Deputies "struggling," finding help after school shooting response
Date: Tuesday, December 7, 2021 6:03:09 PM

December 7, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES

Police chief 'disappointed' his city will host trial of 4 ex-cops in George Floyd's death

St. Paul officials cited safety concerns and security expenses required for the new venue

Video: Denver cop talks suspect into surrender, prevents his suicide

Sheriff: After responding to Oxford High shooting, deputies 'struggling,' finding help

Oakland to vote on $50K police hiring incentive targeting veteran officers

Minn. city to vote on $1.3M plan for alternative public safety programs

Man to face capital murder charge in killing of Texas cop

RIMS Integrated Public Safety Software

Providing dependable software to public safety agencies.

Learn more about our integrated applications for public safety

Leverage ALPR During Assignments with Rekor Blue™

Use Rekor Blue™ for extremely portable and easy-to-use license plate data capture during walking patrols, scene investigations, and covert operations.

Rekor Blue™ 60-day free trial

#TRAININGTUESDAY



Sentinel event review identifies lessons learned from Madison Police Department response to 2020's police protests

By Lt. Dan Marcou

If you wish to prepare your agency for unrest it would behoove you to read the entire report



What cops can learn from YouTube

By Warren Wilson

Seek out as much information from vetted sources as you can, but always ensure any technique, tactic or equipment is in compliance with your agency's policies

ASP Steel Bow Ankle Cuffs



The ASP Steel Bow Ankle Cuffs come with an innovative design and construction features that can revolutionize the restraint industry. Its assorted features set it apart from all other leg restraints available in the market.

Take advantage of our quantity special

ADANI Systems Checkpoint Security Promotion



Includes BV 6045DV X-Ray Baggage Inspection Systems, CEIA PD240 Hand-Held Metal Detector, and CEIA HI-PE Plus Enhanced Walk-Through Multi-Zone Metal Detector. Delivered and installed with 2-year warranty.

Learn more

TIP TUESDAY

Simple hacks to embrace fitness every day

By Eric Tung

Easily build exercise into your daily routine





6 reasons tactical disengagement and redeployment is not 'running away'

By Chief Joel F. Shults, Ed.D.

Tactical redeployment is a strategic tool that should be in our tool kit



SPONSORED CONTENT



Identify narcotics more safely during the opioid crisis third wave

Narcotics detection devices can help law enforcement positively identify unknown substances without exposure.



FEATURED JOB



Sheriff's Deputy-Coroner II - Lateral Job

Apply now!

FEATURED RESOURCES



Grant Funding 101: A Beginner's Guide

Download this beginner's guide to get you up to speed on the basics of understanding how you can best prepare your department to submit a competitive application.



Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Fallen LEO"s family sues alleged killer; Police COVID deaths
Date: Tuesday, September 7, 2021 3:39:28 PM

September 7, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

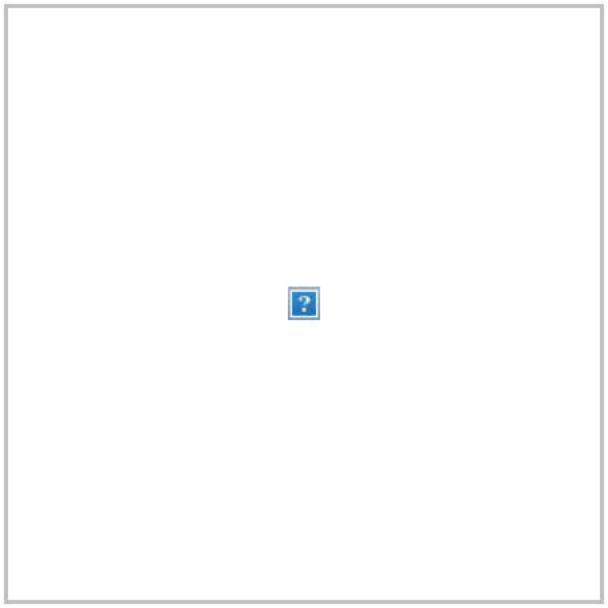
It's just three years old, but the National Law Enforcement Museum opened for the second time on Friday, August 27. Having been closed due to the COVID-19 pandemic, the Museum used the downtime to bring compelling new exhibits and offer more interactive experiences.

"Post 9/11: The Evolution of American Law Enforcement" is the theme of the newest exhibit, which tells the story of how the policing profession has evolved since 9/11/2001. We detail what is on display as part of Police1's 9/11: Reflections at 20 Years coverage, sponsored by Verizon.

Stay safe,

— The Police1 Team

TOP STORIES



COVID deaths impacting police agencies nationwide

The Officer Down Memorial Page reports 132 members of law enforcement agencies are known to have died of COVID-19 in 2021 to date

Video: NYPD officers try to save family from flooded basement apartment after Ida

Judge rejects Minneapolis ballot language on policing

Motive for Florida family's massacre may never be known

Estate of fallen Fla. police officer sues his accused killer for $5M

R.I. mayor appoints civilian to major's post; Black police association objects

The 2021 Motorola Solutions Law Enforcement Survey Results

Gain critical insights from fellow law enforcement officers across the country, highlighting how unifying communications, software, and video technology can ensure transparency and result in enhanced public safety.

Download Survey Report

Rekor Finder: Powerful & Discrete in-vehicle ALPR

Finder is a cost effective in-vehicle ALPR solution that accurately identifies license plates and vehicles in real-time, at high speeds and extreme angles.

Learn More

9/11 ANNIVERSARY

9/11 exhibit newest addition to National Law Enforcement Museum

By Lauri Stevens

The exhibit recognizes the 72 officers killed on September 11, as well as 236 officers who died of illnesses contracted while working in the hazardous conditions at the WTC

LEOs respond: 20 years later, what are the lasting impacts of the September 11 attacks?

By Police1 Staff

Readers and columnists share their thoughts as we prepare to commemorate the 20th anniversary of the terrorist attacks on our nation

SteraMist® Premium Disinfection for Police Stations & Vehicles

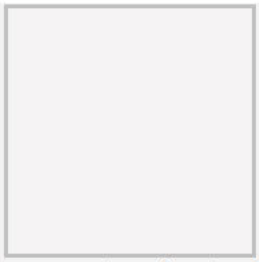
Powered by a sole-active ingredient of 7.8% hydrogen peroxide, SteraMist's

Expand your radio reach by integrating smartphones into your existing system

With the Tango Tango integration service, first responders can connect their existing


ionized Hydrogen Peroxide (iHP™) delivers a powerful high-log disinfection within any area with incredible speed, ease, and superior material compatibility.

Discover SteraMist Disinfection Today!


two-way radio networks with smartphones to augment and extend communications across platforms, channels and agencies.

Learn more

9/11 REFLECTIONS

9/11 reflections: Cops who traded their lives for our freedom

By John M. Lambkin

An NYPD sergeant shares the memories of his friends who willingly ran into the burning towers and participated in the largest rescue mission ever in the history of New York City

Beneath the Vest: How cumulative PTSD impacted a New York cop after 9/11

By Police1 Staff

A former NYPD officer discusses how repeated exposure to trauma took its toll on his mental health and his family

SPONSORED CONTENT

Get more for your money with an all-in-one speaker microphone

This device allows you to reconfigure your mic setup with the slide of a switch, offering flexibility for different situations at a reasonable cost.

FEATURED EDUCATION

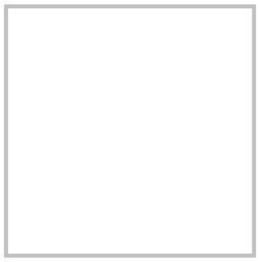
University of Cincinnati Online

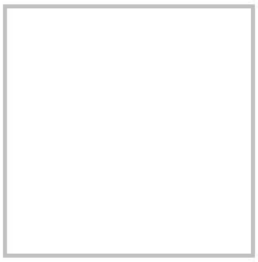
100% online Bachelor's & Master's in Criminal Justice programs. Learn more!

FEATURED DEAL

Tough Is Easy. Tailored Is Critical.

See why Zebra rugged tablets are made for the public safety sector.





Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp Alert
To: Tulipano, Michael (POL)
Subject: Find Grant Money to Fund License Plate Readers
Date: Tuesday, May 18, 2021 8:20:30 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile and covert plate readers, plus our newly released ELSAG Video Plate Hunter 900, a low-cost option for tight budgets.

These force-multiplying systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Irwin, Patrick (POL)
Subject: Find Grant Money to Fund License Plate Readers
Date: Tuesday, May 18, 2021 8:17:01 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile and covert plate readers, plus our newly released ELSAG Video Plate Hunter 900, a low-cost option for tight budgets.

These force-multiplying systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Tapis, Stephen C (POL)
Subject: Find Grant Money to Fund License Plate Readers
Date: Tuesday, May 18, 2021 8:16:51 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile and covert plate readers, plus our newly released ELSAG Video Plate Hunter 900, a low-cost option for tight budgets.

These force-multiplying systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Cronin, John E (POL)
Subject: Find Grant Money to Fund License Plate Readers
Date: Tuesday, May 18, 2021 8:15:59 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile and covert plate readers, plus our newly released ELSAG Video Plate Hunter 900, a low-cost option for tight budgets.

These force-multiplying systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: PoliceGrantsHelp Alert
To: Tulipano, Michael (POL)
Subject: Find Grant Money to Fund License Plate Readers
Date: Tuesday, September 21, 2021 10:46:48 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Our solutions include fixed, mobile and covert plate readers, plus our newly released ELSAG Video Plate Hunter 900, a low-cost option for tight budgets.

These force-multiplying systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help



For information about ELSAG Plate Hunter ® ALPR systems, visit **leonardocompany-us.com.**

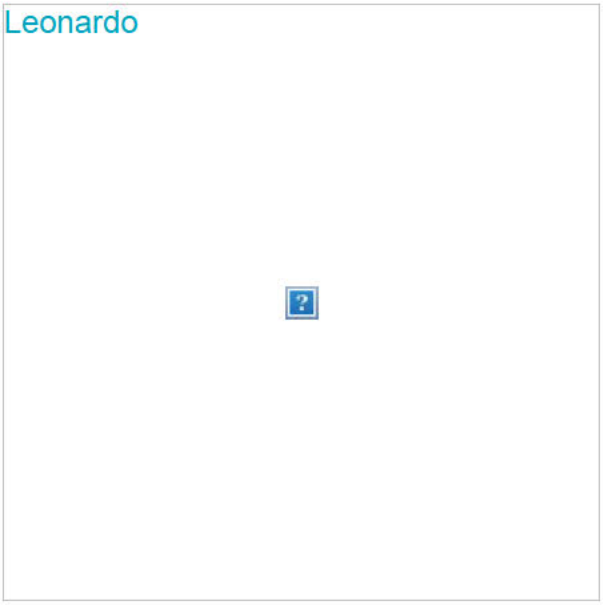
Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: Craig Duncan
To: Foley, James (POL)
Subject: Follow up to NIC
Date: Wednesday, August 18, 2021 12:21:03 PM

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

Leonardo



Hello.
Thanks for stopping by the Leonardo/ELSAG LPR Solutions Booth at the NIC. We hope you had a great conference.

Congratulations to Grady McCraw of NCSHP, who was the winner of the drawing for the Leonardo cooler!

Leonardo has been serving U.S. Law Enforcement LPR needs since 2008. We are committed to providing law enforcement with the best ecosystem of LPR products, 24/7 support, and customer service in the industry.

Our affiliations with the Houston and Atlanta HIDTA LPR and DEA DEASIL LPR networks is a powerful force multiplier for our customers:

The HIDTA ALPR Network includes:

- No ongoing user licenses or user fees

- Over 8000 active law enforcement users
- Over two thousand cameras in network
- Over 1 billion records and growing
- NCIC, **HIDTA BOLOS, the DEA CAT 4 hot list**, over 400 state/local hot lists
- 'Private' hot lists available for sensitive investigative needs
- Law Enforcement only, not held on a private company's server

Advantages of our ELSAG LPR System:

- GSA approved, sole source assistance available
- ONE-TIME license fee at initial purchase
- **NO recurring license fees or user fees for data access**
- Mobile, fixed, radar trailers & covert camera options
- First year warranty FREE, extended warranties available
- Powerful, flexible internet-based analytic software for query/cross/convoy searches & mapping capabilities
- **VPH900**, license-based LPR software system turns most HD video cameras into an LPR camera
- Competitive pricing with financing options
- Superior performance, outstanding service, support, 100% U.S- based
- **Free grant assistance** to help you identify federal, state or local grants

I look forward to talking with you and helping you with all of your LPR needs.

Stay safe,
Craig Duncan
Sr. Field Operations Manager - Southeast

PS Watch your inbox for an invite to a webinar on the HIDTA ALPR Network EOC analytics coming soon!

Leonardo Company, 4221 Tudor Lane, Greensboro, North Carolina 27410
Unsubscribe Manage preferences

From: Edward Meade
To: Burns, Timothy (POL)
Subject: Fwd: Internal Automated License Plate Recognition (ALPR) System Scan File Request Form
Date: Friday, December 3, 2021 6:18:37 PM

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

---------- Forwarded message ---------
From: **Google Forms** <forms-receipts-noreply@google.com>
Date: Fri, Dec 3, 2021 at 6:11 PM
Subject: Internal Automated License Plate Recognition (ALPR) System Scan File Request Form
To: <edward.meade@pd.boston.gov>

Thanks for filling out Internal Automated License Plate Recognition (ALPR) System Scan File Request Form

Here's what was received.

Internal Automated License Plate Recognition (ALPR) System Scan File Request Form

Sworn Department personnel of the rank of Sergeant and higher are authorized to make a request to the Technology Services Division for a copy of scan files. ** ALPR DATA IS AUTOMATICALLY PURGED AFTER 30 DAYS ** Special Order 16-031 (http://bpdnet/wordpress/?page_id=13138)

Your email (**edward.meade@pd.boston.gov**) was recorded when you submitted this form.

Your ID *

010128

Rank, First & Last Name *

Sergeant Detective Edward Meade

Your Contact Phone Number

617-594-9293

--
Edward P. Meade
Sergeant Detective
Boston Police Department
Boston Regional Intelligence Center
1 Schroeder Plaza, Boston MA 02120

Edward.Meade@pd.boston.gov

O / 617-343-4328
F / 617-343-5222

Incident Number

Reason for Request *

The employee making the request shall document the reason for the request. Requests may be made only for legitimate law enforcement purposes, as part of normal procedures for investigations and the handling of evidence or in furtherance of the purposes for the ALPR system stated in Special Order 16-031 (http://bpdnet/wordpress/?page_id=13138)

Investigative assist for MSP - SAU Investigation

Requested Date *

MM DD YYYY

11 / 26 / 2021

Start Time and End Time *

Use 24 hour time or specify AM/PM (ie 14:00hrs to 15:00hrs or 2:00pm to 3:00pm)

0000 to 2359 Hrs

Requested ALPR Locations

Choose all that apply

- [ ] (A-1) Tremont Street / Stuart Street
- [ ] (B-2) Blue Hill Ave / Washington Street
- [ ] (B-3) Blue Hill Av / Harvard Street

Other Information

Create your own Google Form
Report Abuse

From: Spatialitics LLC
To: Wilczynski, Kristin (POL)
Subject: GeoShield: Monitor Your City in Real-Time with Live Video Streaming
Date: Tuesday, May 18, 2021 1:10:53 PM

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

What's New Banner

Monitor Your City in Real-Time with Live Video Streaming

GeoShield updates for 2021 include key enhancements focused on Video Streaming and User Experience. A few of these features & enhancements include:

Reduced Video Latency

REDUCED VIDEO LATENCY

GeoShield Unity Connector and Real Time Video Streaming have reduced latency on RTSP Streaming Video Streams under 500 milliseconds.

Agency Identity Authentication

AGENCY IDENTITY AUTHENTICATION

GeoShield now supports Azure Active Directory and ArcGIS Identity Store, allowing agencies to manage their users and access GeoShield with agency provided credentials.

Real Time Information Access

REAL-TIME INFORMATION ACCESS

Improvements in GeoShield Unity Connector to better handle data; supporting deleted records, incremental updates, and batch reconciliation to always keep your data updated.

Enhanced User Experience

ENHANCED USER EXPERIENCE

Updates for increased data transparency for the end user, providing information on loading data and video streams. Enhancements to Crime Analysis dashboards to easily sort and filter crime data.

« COMING UP IN NEXT RELEASE »

- LPR Notification support from FLOCK ALPR and Vigilant ALPR
- Advanced filtering within the table and associated mapping results for in-depth analysis
- Additional chart types to visualize data in attractive and intuitive ways

& much more...

At Spatialitics, we are continuously improving our solutions based on our client needs and feedback. We are looking for ways to make our solutions simple and efficient. The above enhancements were provided to make policing convenient for you and to assist you in keeping your community safe.

A Force Multiplier designed for your Agency

Ask for a free GeoShield Demo now!!

Request a Demo



Spatialitics

This email and any offer considered in this document are brought to you by **Spatialitics LLC**
To unsubscribe from this mailing list, **click here**

From: Spatialitics LLC
To: Fitzgerald, Carol (POL)
Subject: GeoShield: Monitor Your City in Real-Time with Live Video Streaming
Date: Tuesday, May 18, 2021 1:10:57 PM

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

What's New Banner

Monitor Your City in Real-Time with Live Video Streaming

GeoShield updates for 2021 include key enhancements focused on Video Streaming and User Experience. A few of these features & enhancements include:

Reduced Video Latency

REDUCED VIDEO LATENCY

GeoShield Unity Connector and Real Time Video Streaming have reduced latency on RTSP Streaming Video Streams under 500 milliseconds.

Agency Identity Authentication

AGENCY IDENTITY AUTHENTICATION

GeoShield now supports Azure Active Directory and ArcGIS Identity Store, allowing agencies to manage their users and access GeoShield with agency provided credentials.

Real Time Information Access

REAL-TIME INFORMATION ACCESS

Improvements in GeoShield Unity Connector to better handle data; supporting deleted records, incremental updates, and batch reconciliation to always keep your data updated.

Enhanced User Experience

ENHANCED USER EXPERIENCE

Updates for increased data transparency for the end user, providing information on loading data and video streams. Enhancements to Crime Analysis dashboards to easily sort and filter crime data.

« COMING UP IN NEXT RELEASE »

- LPR Notification support from FLOCK ALPR and Vigilant ALPR
- Advanced filtering within the table and associated mapping results for in-depth analysis
- Additional chart types to visualize data in attractive and intuitive ways

& much more...

At Spatialitics, we are continuously improving our solutions based on our client needs and feedback. We are looking for ways to make our solutions simple and efficient. The above enhancements were provided to make policing convenient for you and to assist you in keeping your community safe.

A Force Multiplier designed for your Agency

Ask for a free GeoShield Demo now!!

Request a Demo



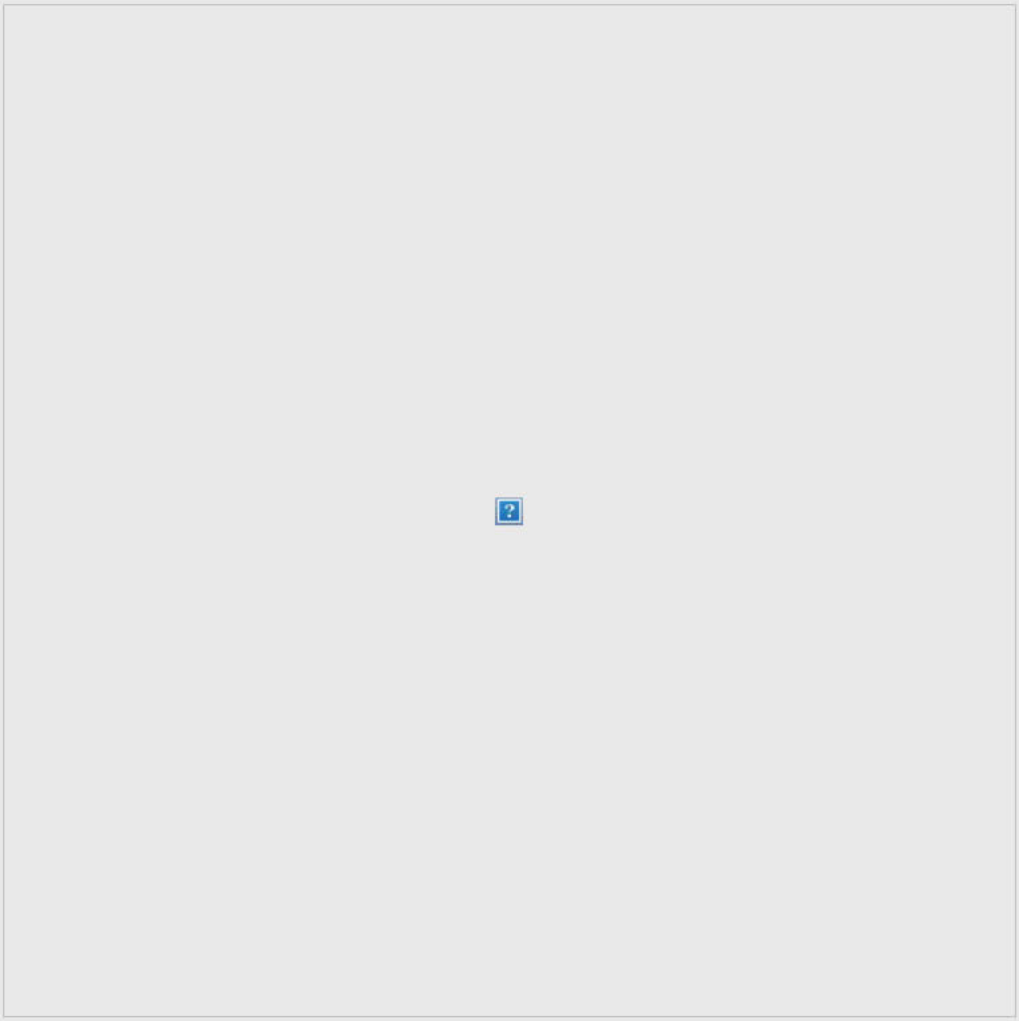
Spatialitics

This email and any offer considered in this document are brought to you by **Spatialitics LLC**
To unsubscribe from this mailing list, **click here**

From: POLICE
To: Hackett, John (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 21, 2021 12:31:50 PM

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

Nov 21, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

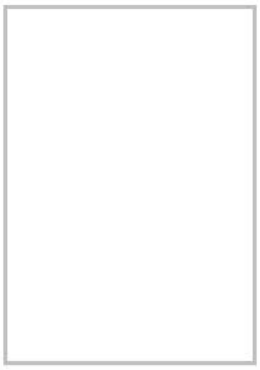
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as john.hackett@massmail.state.ma.us. Manage your email preferences.

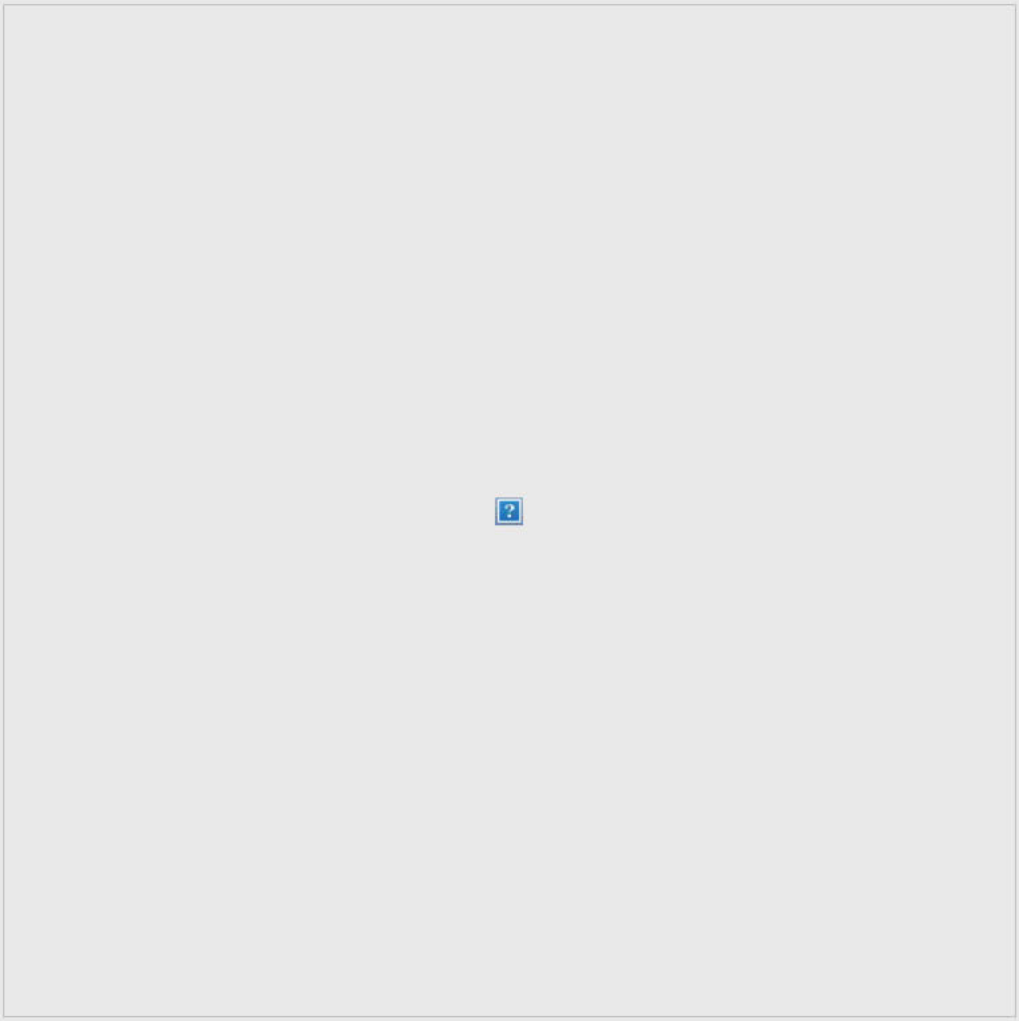
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Rizos_Byron (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 21, 2021 12:31:50 PM

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

Nov 21, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

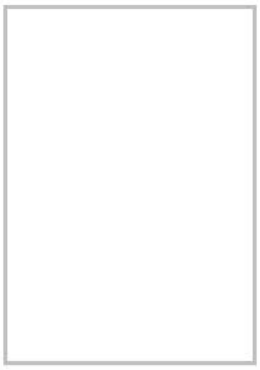
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as byron.rizos@pol.state.ma.us. Manage your email preferences.

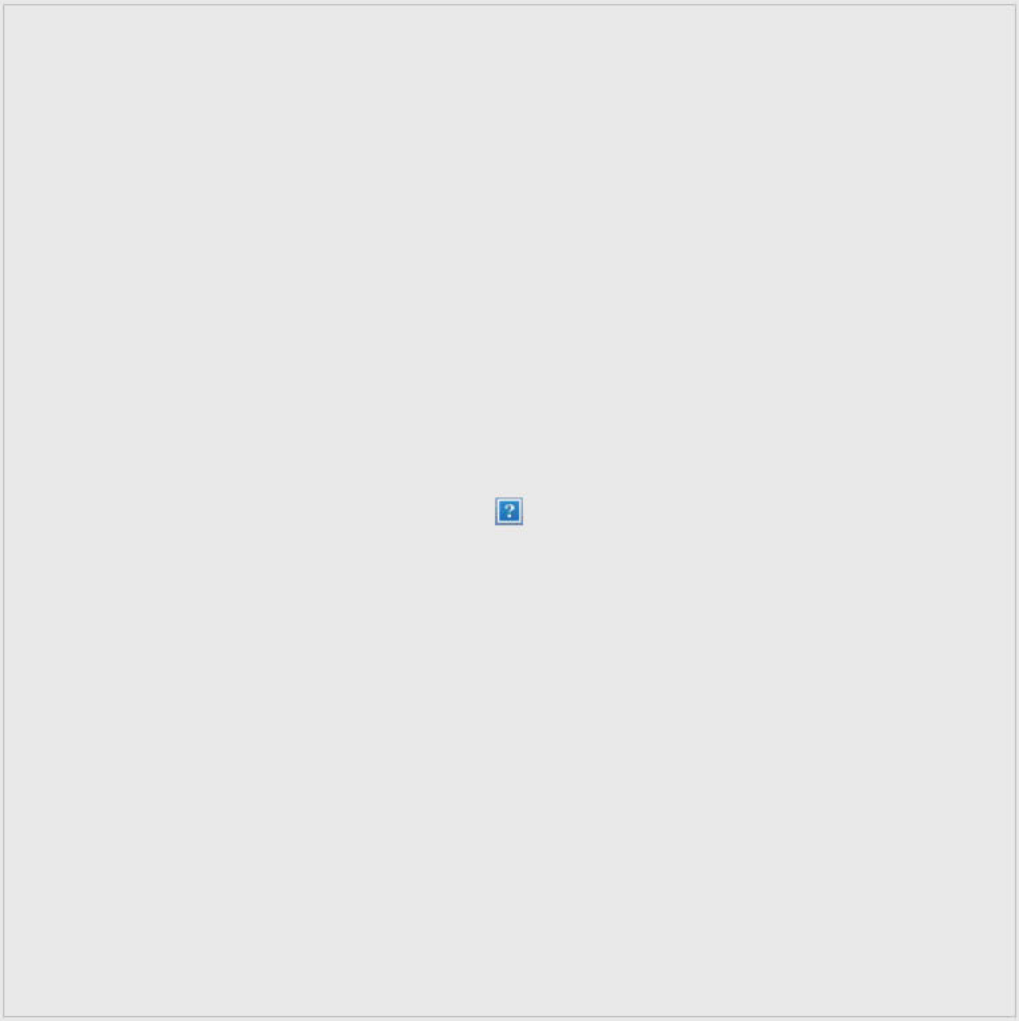
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Gamari James (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 21, 2021 12:31:49 PM

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

Nov 21, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

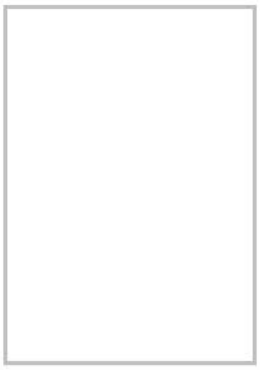
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as james gamari@pol.state.ma.us. Manage your email preferences.

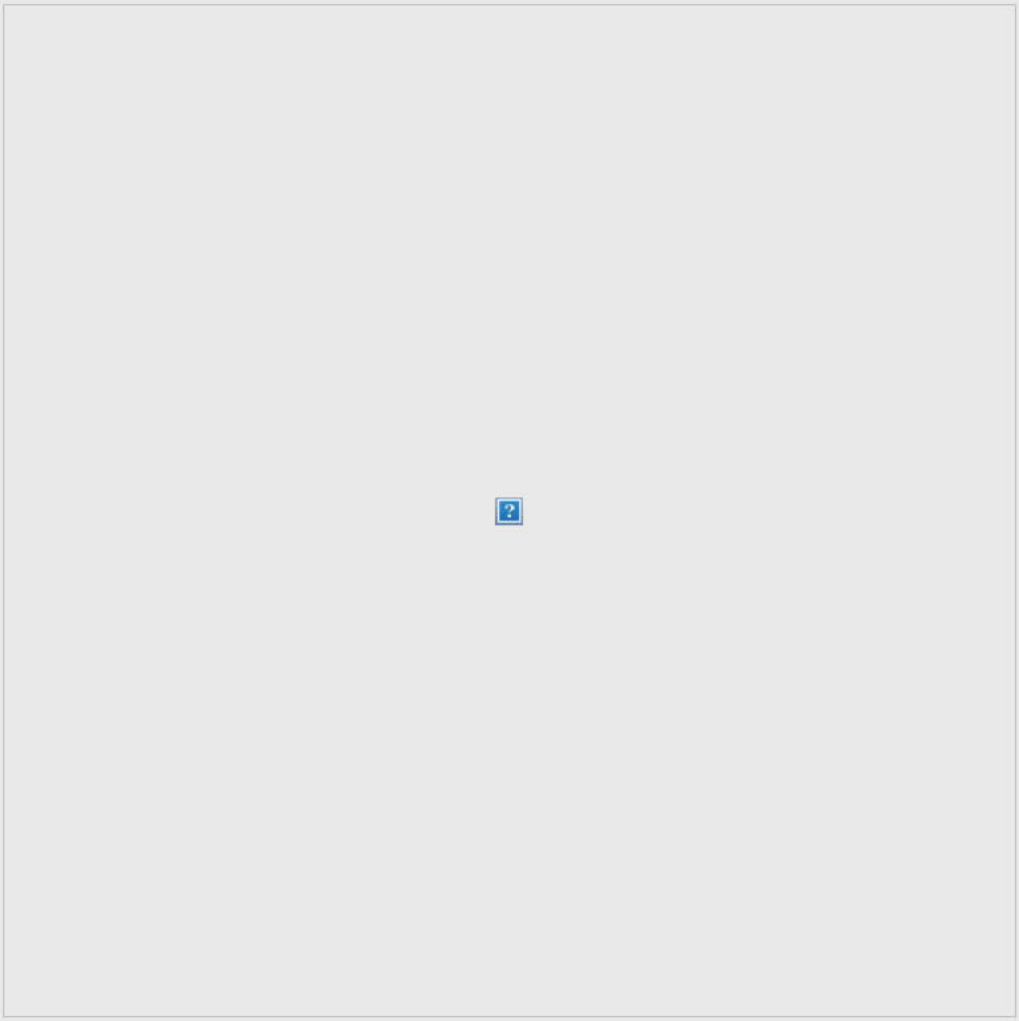
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Bakey Thomas (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 21, 2021 12:31:49 PM

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

Nov 21, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

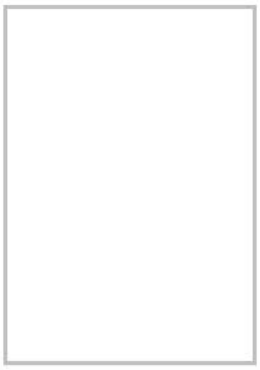
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as homas.bakey@pol.state.ma.us. Manage your email preferences.

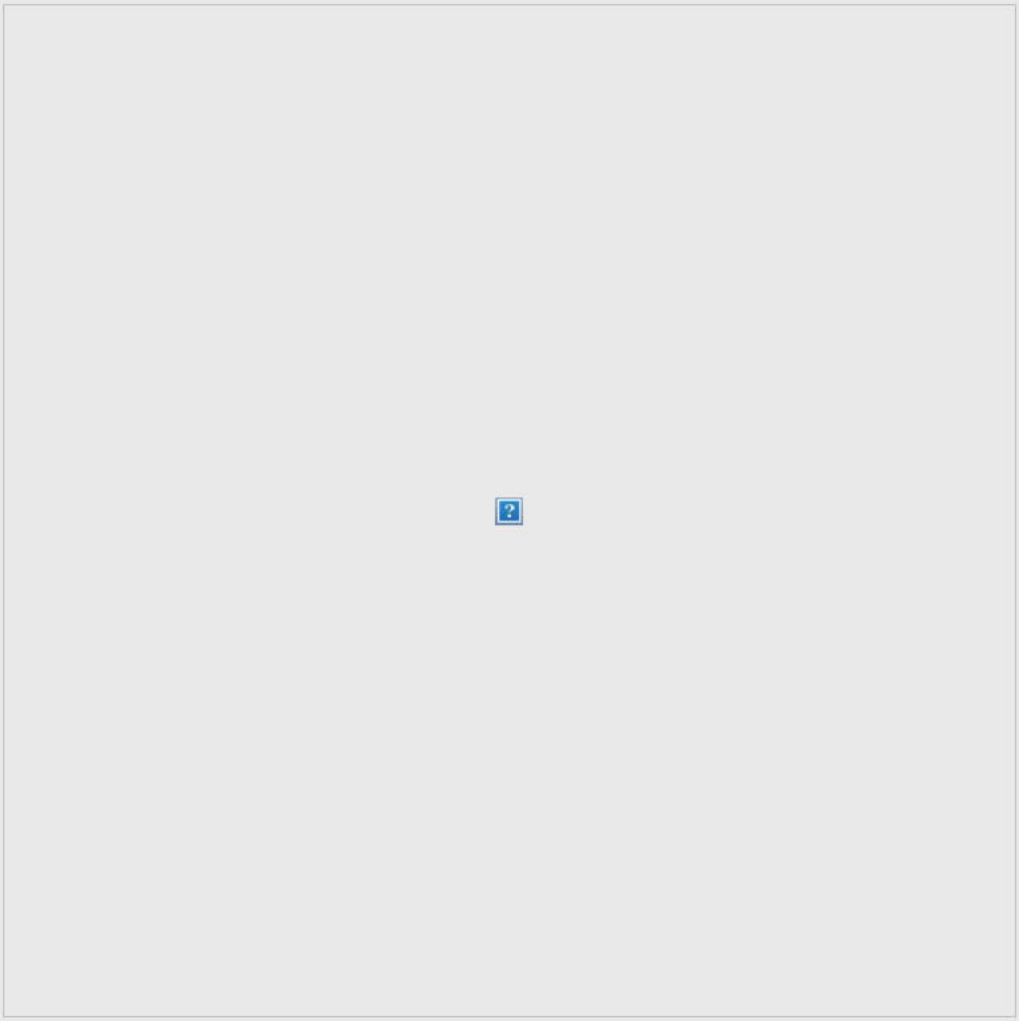
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Mormino_Matthew (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 21, 2021 12:31:48 PM

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

Nov 21, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

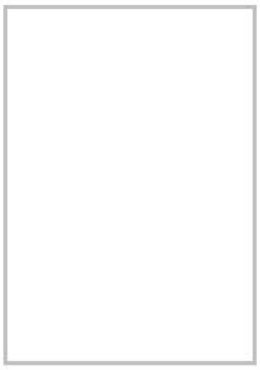
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as matthew.mormino@pol.state.ma.us. Manage your email preferences.

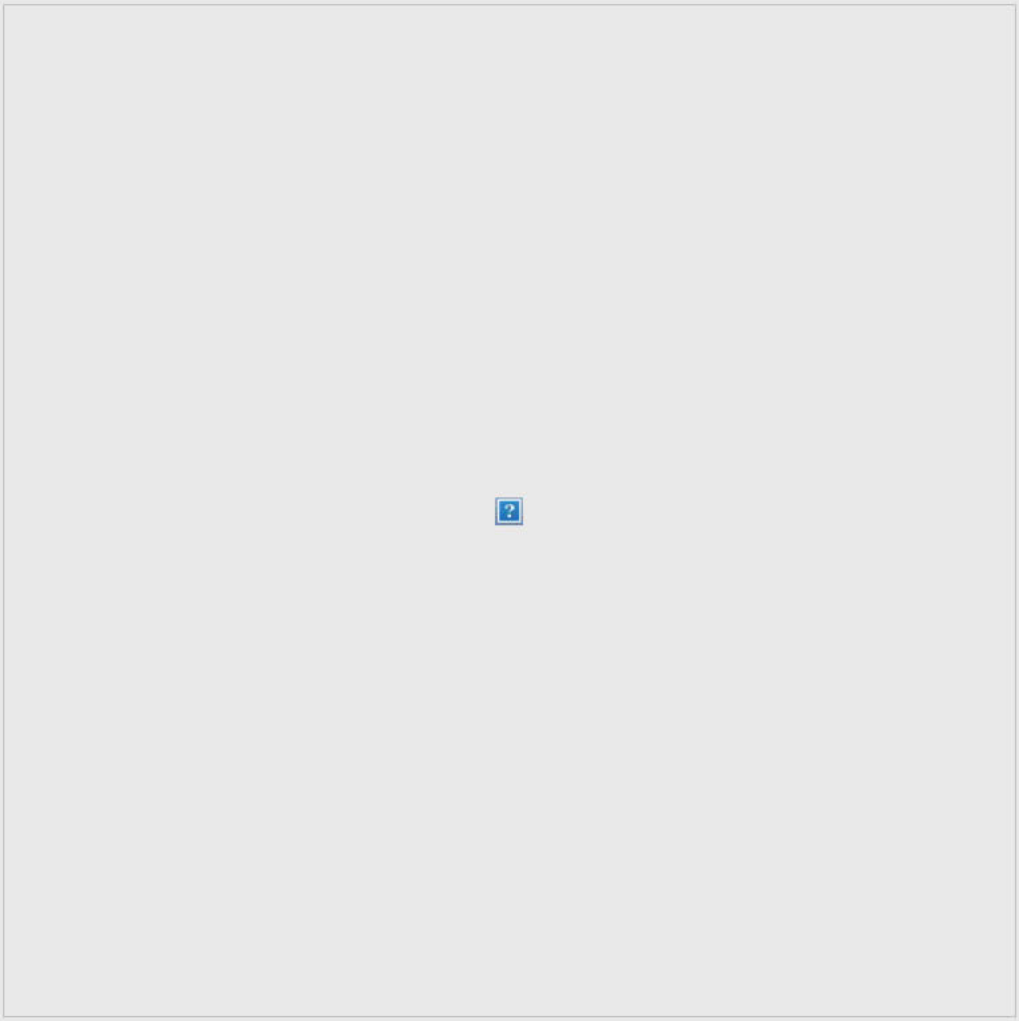
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Brenner, Karl (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 7, 2021 12:32:07 PM

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

Nov 7, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

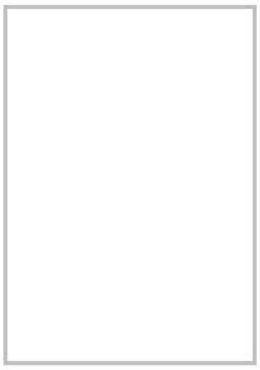
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as karl.brenner@state.ma.us. Manage your email preferences.

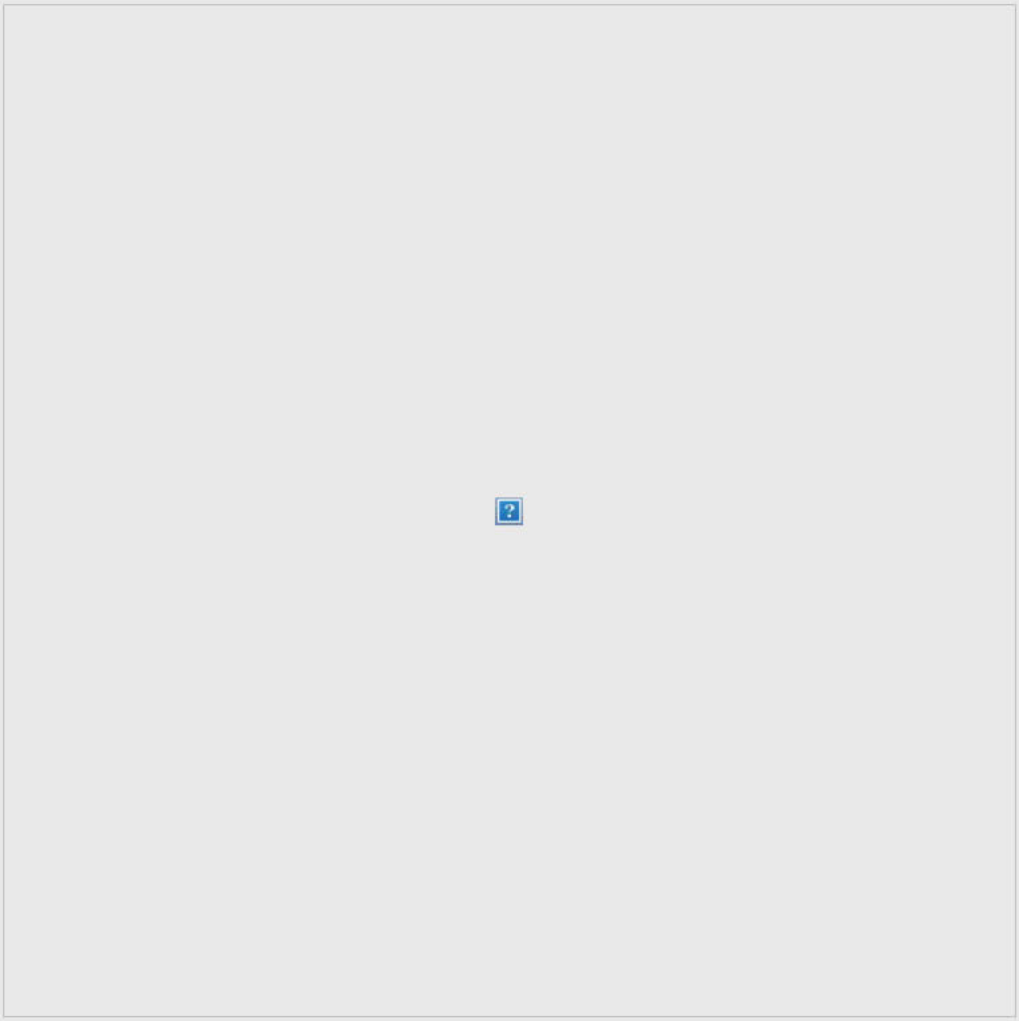
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Gamari James (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 7, 2021 12:32:05 PM

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

Nov 7, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

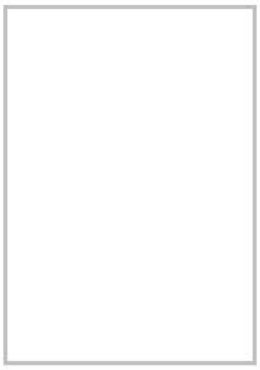
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD



Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as james gamari@pol.state.ma.us. Manage your email preferences.

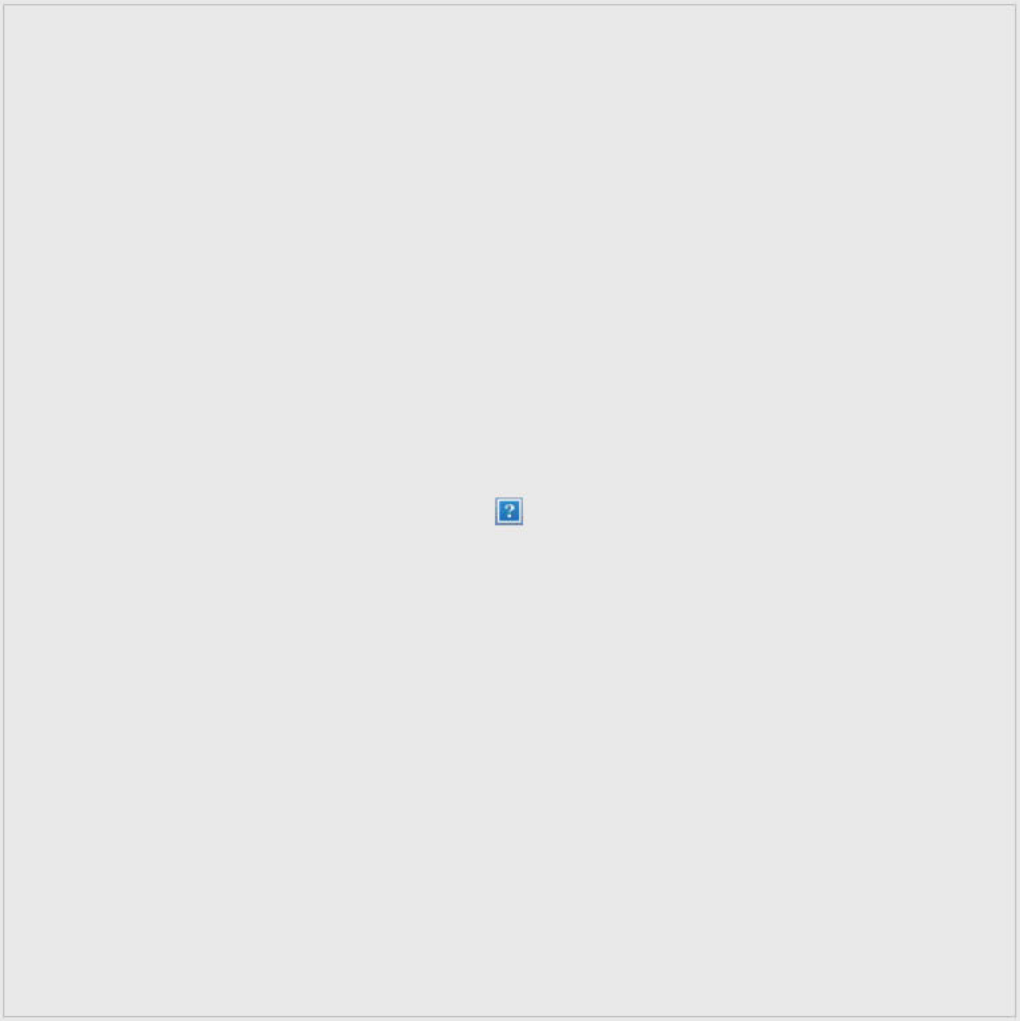
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Hackett, John (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 7, 2021 12:31:54 PM

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

Nov 7, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD



Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD



Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

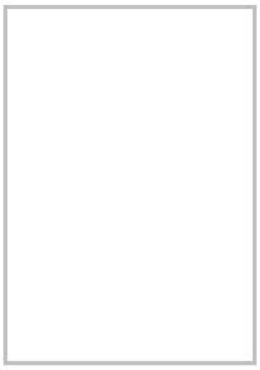
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as john.hackett@massmail.state.ma.us. Manage your email preferences.

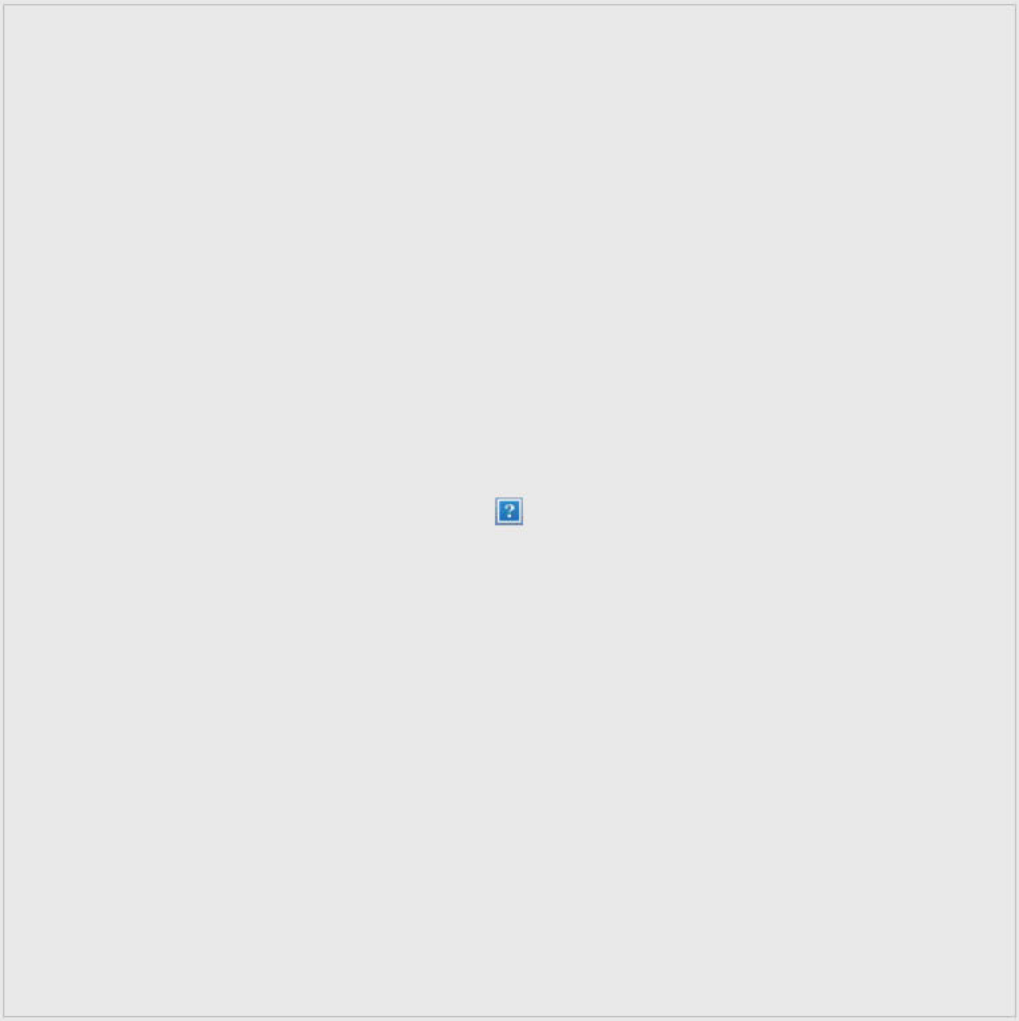
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Mormino, Matthew (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 7, 2021 12:31:51 PM

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

Nov 7, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

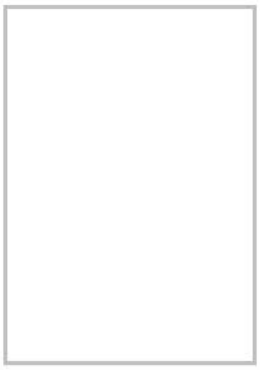
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as matthew.mormino@pol.state.ma.us. Manage your email preferences.

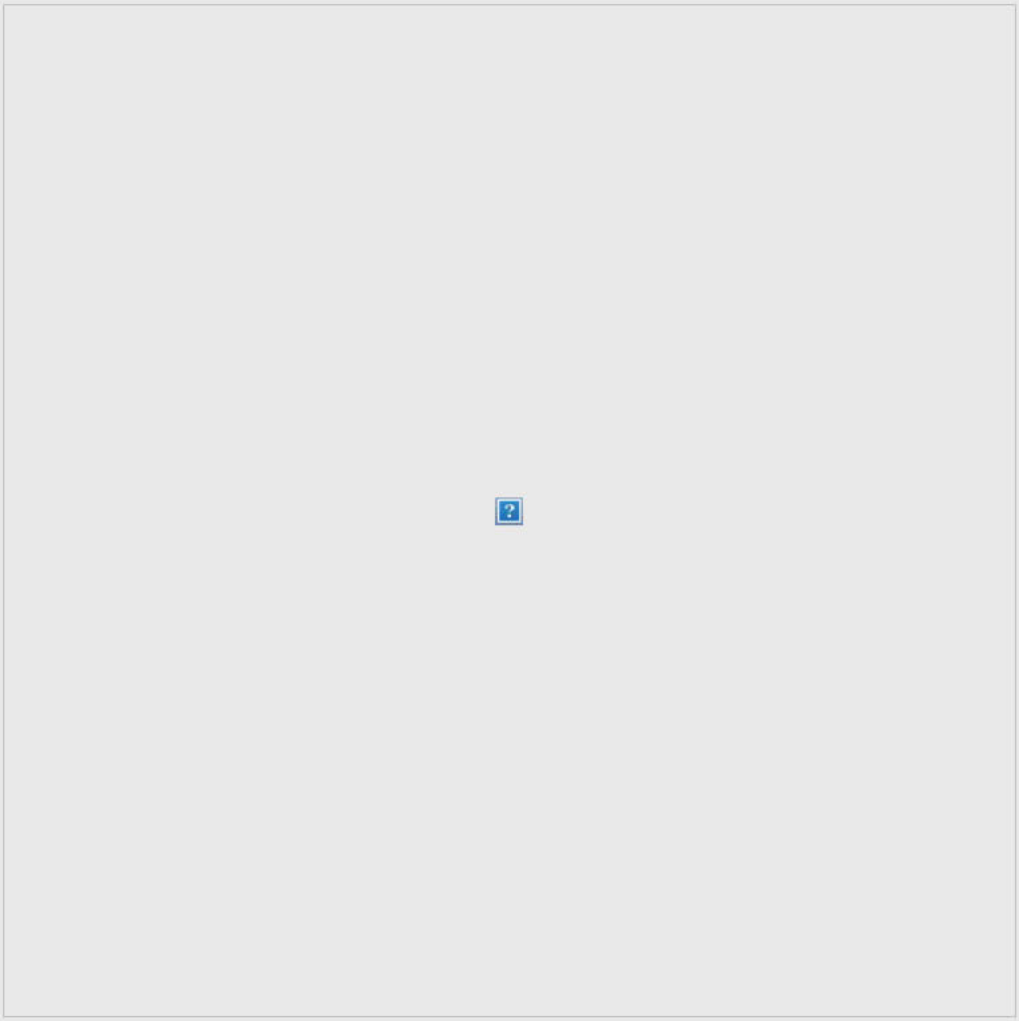
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Rizos_Byron (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 7, 2021 12:31:49 PM

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

Nov 7, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

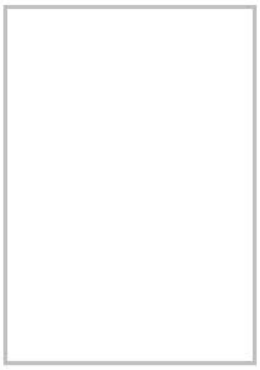
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as byron.rizos@pol.state.ma.us. Manage your email preferences.

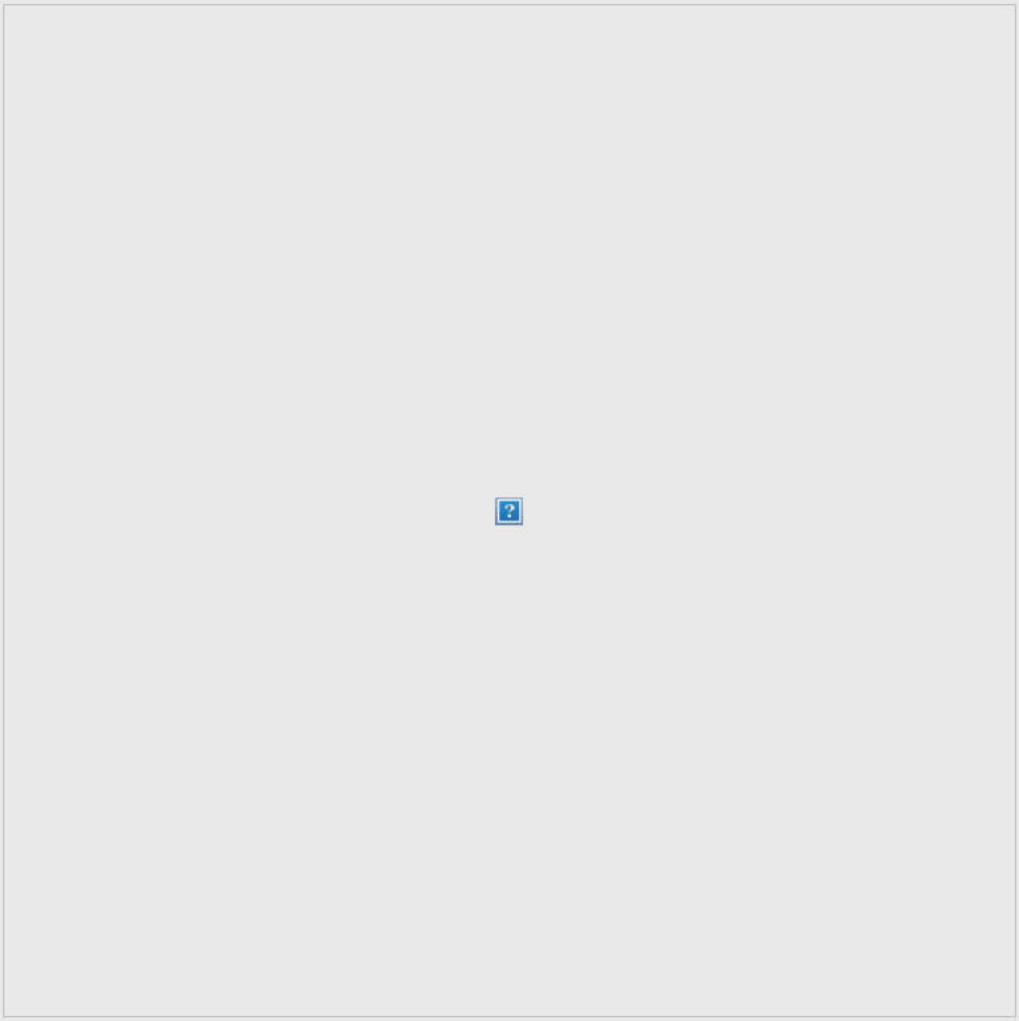
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Brenner, Karl (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, November 1, 2021 1:12:27 PM

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

Nov 1, 2021



FREE WHITEPAPERS

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD

Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

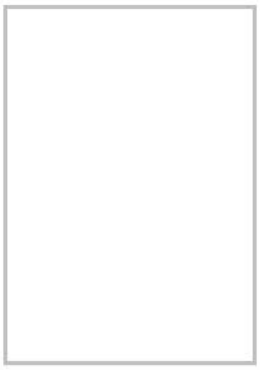
DOWNLOAD

Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD





Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD



Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as karl.brenner@state.ma.us. Manage your email preferences.

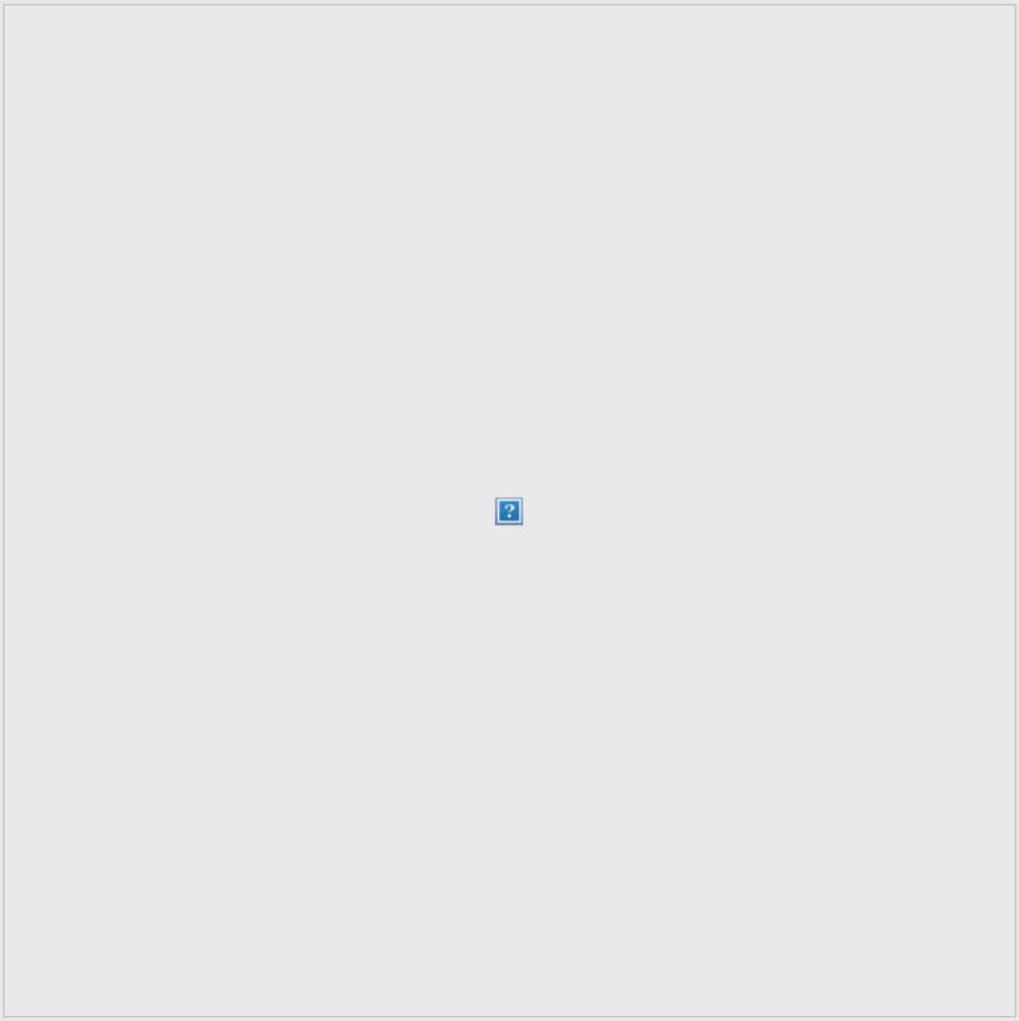
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Gamari James (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, November 1, 2021 1:10:56 PM

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

Nov 1, 2021



FREE WHITEPAPERS

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD

Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

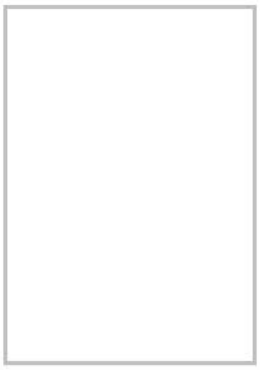
DOWNLOAD

Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD





Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD



Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as james gamari@pol.state.ma.us. Manage your email preferences.

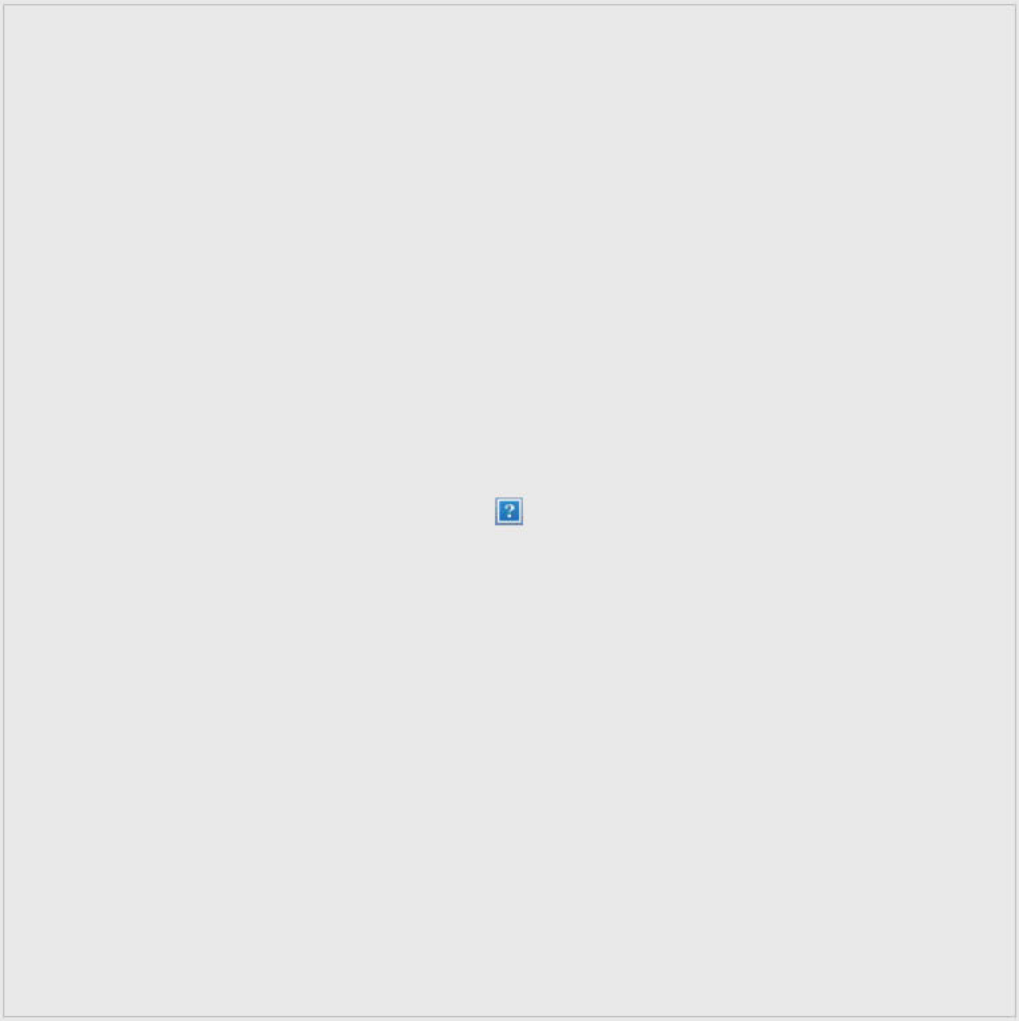
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Rizos, Byron (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, November 1, 2021 1:10:43 PM

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

Nov 1, 2021

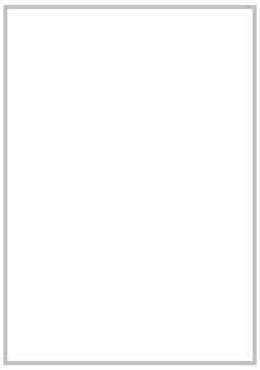


FREE WHITEPAPERS

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.



DOWNLOAD



Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD



Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD

Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD

Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as byron.rizos@pol.state.ma.us. Manage your email preferences.

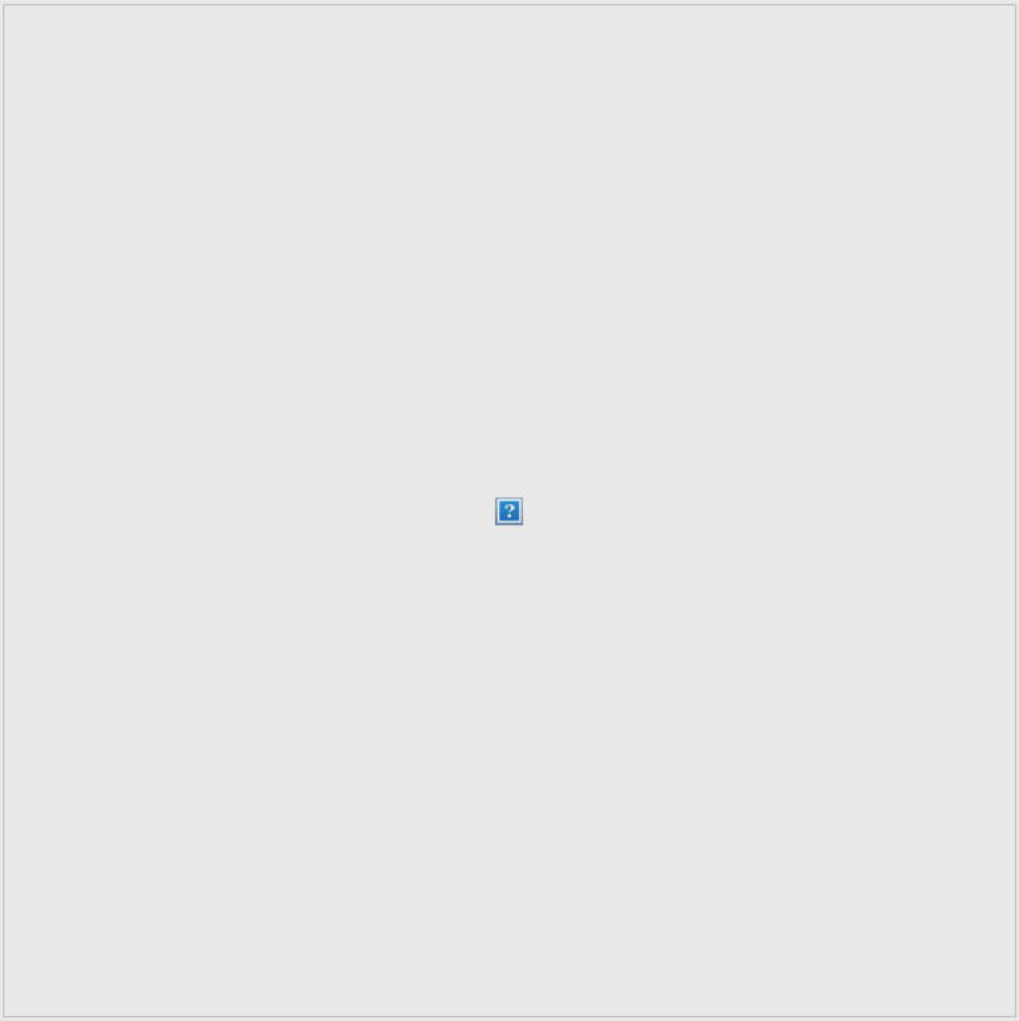
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Mormino_Matthew (POL)
Subject: Get POLICE"s Top How-To"s
Date: Monday, November 1, 2021 1:10:36 PM

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

Nov 1, 2021



FREE WHITEPAPERS

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD

Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

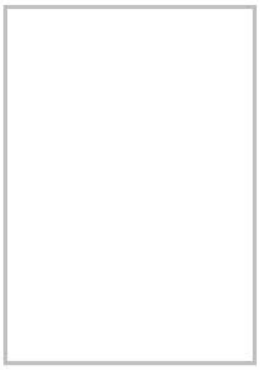
DOWNLOAD

Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD





Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD



Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as matthew.mormino@pol.state.ma.us. Manage your email preferences.

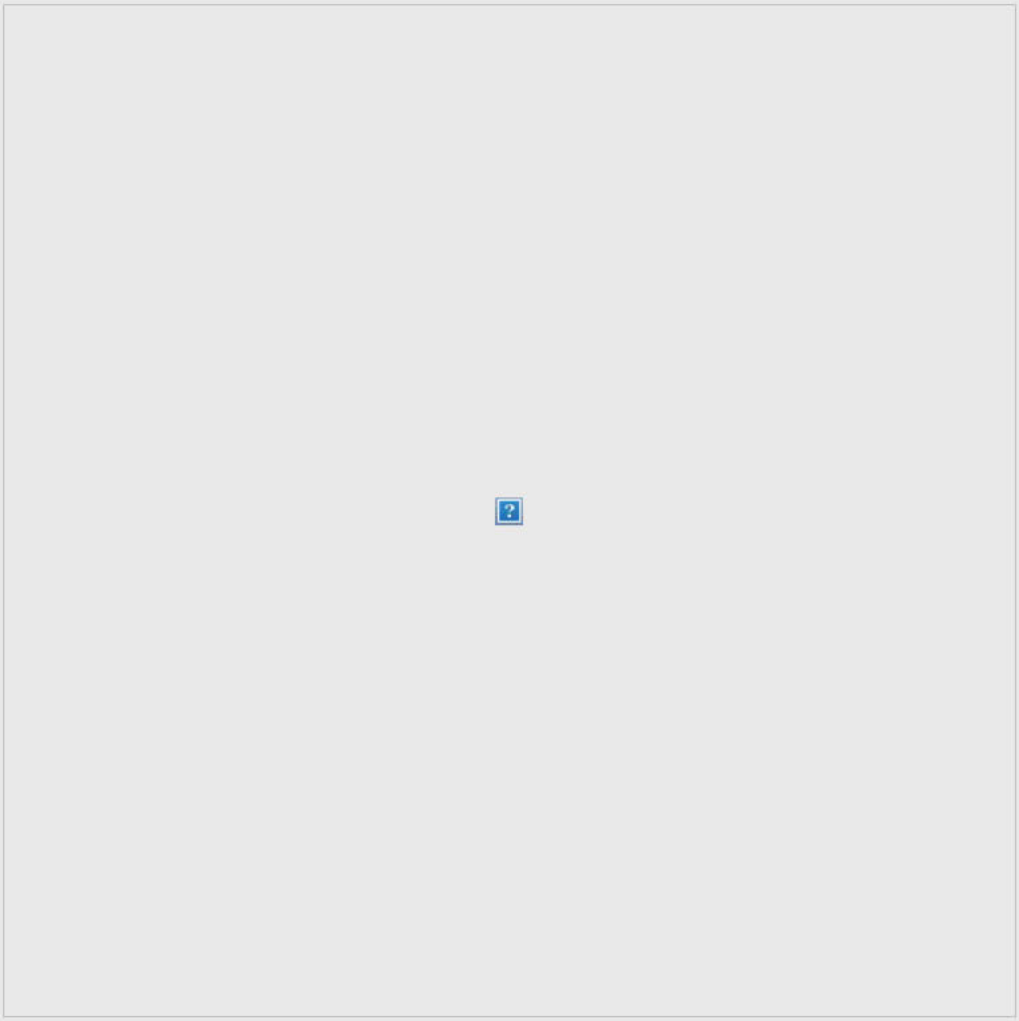
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: POLICE
To: Brenner, Karl (POL)
Subject: Get POLICE"s Top How-To"s
Date: Sunday, November 21, 2021 12:31:58 PM

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

Nov 21, 2021



FREE WHITEPAPERS

Sponsored by Knott Laboratory

Digital Media Forensics & Vehicle-Related Officer Involved Shootings: Critical Incident Scene Reconstruction

When a critical incident occurs, most law enforcement agencies do not have the resources, staff, and training to perform in-depth analysis on the digital evidence associated with each case. And yet, these pieces of digital evidence can end up in the media to be tried by the court of public opinion.

DOWNLOAD

Sponsored by Leonardo

LPR Technology: A Solution for Law Enforcement Agencies Facing National Scrutiny, Decreased Budgets, and High Officer Attrition

It is a challenging time for law enforcement agencies nationwide. Now more than ever before, officers need to have access to technology that promotes equitable policing while increasing the safety of their communities. This whitepaper explores one example of this technology: license plate readers.

DOWNLOAD

Sponsored by Magnet Forensics

A New Paradigm in Digital Investigations

Digital evidence has become integral to solving crimes today, but agencies are often overwhelmed with the volume of data – causing major challenges for labs and agencies around the world.

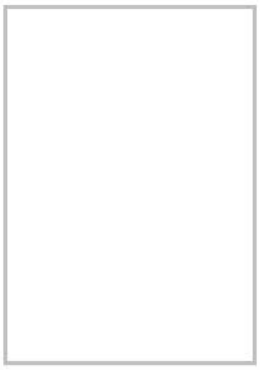
DOWNLOAD

Sponsored by POLICE

Special Report: The Future of Firearms Training 2022

In the POLICE Special Report: The Future of Firearms Training 2022 read about how virtual reality technology is being used in simulator training, how some agencies are adding scenario training to their live-fire ranges, and what can be done to minimize gunfire noise disturbing people who live near police firing ranges.

DOWNLOAD





Sponsored by POLICE

Special Report: Innovations in Police Technologies for 2022

In the POLICE Special Report: Innovations in Police Technologies for 2022, read about the latest law enforcement solutions in digital forensics from Magnet Forensics, eCitation from Brother Mobile Solutions, records management from CentralSquare Technologies, digital video evidence from Veritone, and communications from Wireless Pacific.

DOWNLOAD



Sponsored by POLICE

Special Report: Mobile Tech Innovations

In the POLICE Special Report: Mobile Tech Innovations, read about DH Wireless Solutions' Portable Data Network systems, Jenoptik's highly advanced mobile ALPR technology, and LexisNexis' Coplogic Ethos cloud-based data management and optimization platform.

DOWNLOAD



Sponsored by Amplivox Sound Systems, BlueRidge Armor, Hardwire LLC, Johnson Controls, Nuance Communications, Ring Power

Special Report: Critical Incident Response

In POLICE Magazine's Special Report: Critical Incident Response, read about Working with the Media After a Critical Incident, the Evolution of Critical Incident Communications, Bomb Threats and Suspicious Packages, Preplanning Response to School Shootings, and PTSD in the Police K-9.

DOWNLOAD

Sponsored by Hardwire LLC, Gamber-Johnson LLC, Code 3 Inc., Derive Systems, DEW Engineering & Developement ULC, Pursuit Emergency Vehicles, CTech Manufacturing

Special Report: Upfitting & Fleet Management

In POLICE Magazine's Special Report: Upfitting & Fleet Management, learn about whether do to Upfitting In-House or Outsource, Bringing Maintenance In House, 10 CHP's Vehicle Assembly Line, Telematics for Law Enforcement, and Hybrids Ready for Patrol.

DOWNLOAD

VIEW MORE FREE WHITEPAPERS

POLICE MAGAZINE

You are currently subscribed as karl.brenner@state.ma.us. Manage your email preferences.

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

Contact Us | Privacy Policy | Unsubscribe

From: IUPA NewsWatch
To: Davis, Matthew (POL)
Subject: Give your dad the chance to win a Harley for Father"s Day while helping LEOs and their families!
Date: Tuesday, June 15, 2021 9:32:23 AM

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

This message was sent to matthew.davis@pol.state ma.us
To advertise in this publication please click here

June 15, 2021

Give your dad the chance to win a Harley for Father's Day while helping LEOs and their families!

LEORF News

The Law Enforcement Officers Relief Fund (LEORF) with the assistance of Stinger Harley-Davidson, Medina, OH, is raffling off a brand new 2021 Harley-Davidson® FLHTK Ultra Limited Peace Officer Special Edition in Dark Blue!

READ MORE

'A huge impact': SLCPD Peer Support Group helps break down mental health stigma

ABC4 News

On August 9, 2020, a vehicle went off the road and entered the Jordan River. Two juveniles died in the crash after becoming trapped inside the flipped car. Darren Nichols, a Salt Lake City Police Officer, was the first to arrive at the scene. “I ended up dropping all my gear and jumping in the water in an attempt to save the kids’ lives. The two-year-old was still trapped in the

vehicle at that time and the mom was out of the vehicle, and it was a really, really difficult incident," Nichols told ABC4.

READ MORE

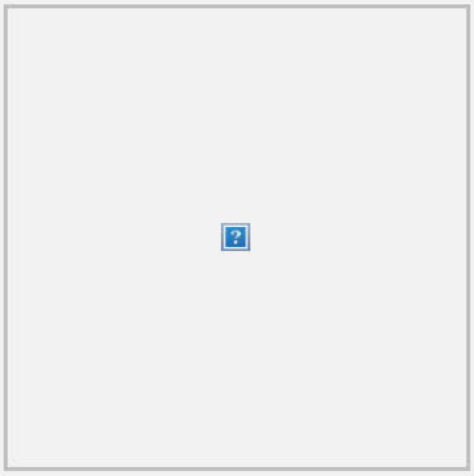
Outpouring of support for LEOs in Port Saint Lucie!

LEORF News

During Police Week 2021, the community of Port Saint Lucie, Florida showed their local law enforcement heroes just how much they truly appreciate them! Lunch was donated by JYD BBQ, breakfast from Aycock Funeral Homes, dinner from Texas Roadhouse, and snacks from Wickshire Port Saint Lucie!

READ MORE

PRODUCT SHOWCASE



Your investigations. Our software.

Today, almost every aspect of our lives can be found on our phones—pictures, locations, activities, conversations, relationships, the list goes on—which is why we provide a unified solution to help you dive into the data of life.

LEARN MORE

History on the walls of the I.U.P.A.

I.U.P.A. Briefing Room

If you walk the halls of the I.U.P.A. Headquarters, you might think you are in a museum. Each hallway is lined with historical pictures, charters, documents, awards, and tokens of appreciation that denote four decades of dedication to the members of the I.U.P.A. and to the law enforcement community as a whole.

READ MORE

'Every different street is a different adventure.' Correctional officer runs across Iowa for fallen coworkers

KWWL News

Ryan Miller has been running a marathon a day, plus biking another 15 miles after that. He sounds like a fitness junkie, but he's actually just a runner using his hobby to make sense of a sudden loss. Miller works as a correctional officer at the Anamosa State Penitentiary where officer Robert McFarland and nurse Lorena Schulte died when two inmates tried to escape on March 23, 2021.

READ MORE

New evidence suggests COVID-19 vaccines remain effective against variants

NPR
The emergence of new and more infectious variants of the coronavirus has raised a troubling question: Will the current crop of COVID-19 vaccine prevent these variants from causing disease? The research was fairly straightforward. Scientists took blood from volunteers who had received the Johnson & Johnson COVID-19 vaccine and looked at the levels of neutralizing antibodies, the kind that prevent a virus from entering cells.

READ MORE

How the American Rescue Plan can help your department fund needed communication equipment purchases

Police 1
The American Rescue Plan is aimed at providing relief for local and state governments and businesses struggling due to COVID-19, as well as to achieve other priorities of the Biden administration and Congress. The $1.9 trillion legislation is in addition to nearly $4 trillion in COVID relief provided in 2020. The ARP provides $350 billion to help states, counties, cities and tr bal governments cover increased expenditures, replenish lost revenue and mitigate economic harm from the COVID-19 pandemic.

READ MORE

Grant: School Violence Prevention Program (SVPP)

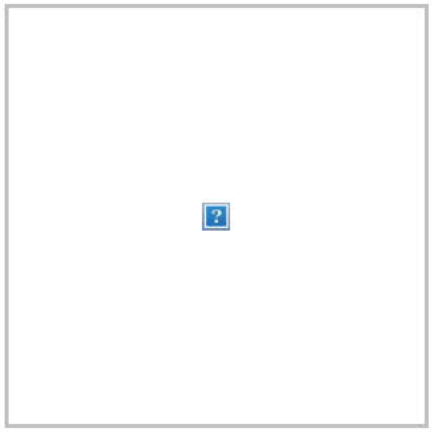
COPS
The Students, Teachers, and Officers Preventing School Violence Act of 2018 (STOP School Violence Act of 2018) gave the COPS Office authority to provide awards directly to States, units of local government, or Indian tr bes to improve security at schools and on school grounds in the jurisdiction of the grantee through evidence-based school safety programs and technology.

READ MORE

Capitol Officer Eugene Goodman to throw first pitch at MLB game

Police 1
Officer Eugene Goodman, who became a household name for his role in defending the U.S. Capitol on January 6, will throw out the first pitch at an upcoming Washington Nationals game. According to NPR, Goodman is expected to throw the ceremonial pitch at the home game on June 18 against the New York Mets.

READ MORE



Rebound: Protecting those who protect us

I.U.P.A. Briefing Room

How one athletic trainer is improving the health and well-being of first responders Luis Rivera saw a problem. A big one. A firefighter in Milwaukee had been struggling with a nagging shoulder injury for more than a year. Rivera, an athletic trainer who worked with elite athletes, had seen this same kind of injury dozens of times before and couldn't believe this firefighter was still in pain.

READ MORE

5 Zoom and webinar presentation tips for LEOs

Police 1

The pandemic has pushed police departments to adopt new procedures and technologies to continue providing community services, as well as to fulfill internal respons bilities like training. One of the most significant and l kely lasting changes has been the widespread use of online technologies like Zoom, GoToWebinar, Google Meet and Microsoft Teams for departmental meetings, training events and community education programs.

READ MORE

Boom: The Eureka Police Department invites you to narc on your illegal fireworks-shooting neighbors using this handy form

Lost Coast Outpost

In response to the growing number of illegal firework complaints over the years (a 137% increase from 2019 to 2020), the City of Eureka has created a new form to report illegal fireworks. The form can be found on the Eureka Police Department website eurekapd.net or here. Completed forms can be submitted by email, mail, or in person and will be reviewed by both Eureka Police and Humboldt Bay Fire.

READ MORE

In Montana, crisis support teams offer alternatives to policing mental health

NPR

By the time Kiki Radermacher, a mental health therapist, arrived at a Missoula, Mont., home on an emergency 911 call in late May, the man who lived there and had called for help was backed into a corner and yelling at police officers. The place he was renting was about to be sold. He had called 911 when his fear of becoming homeless turned to thoughts of killing himself.

READ MORE

Fuel savings, needed power expected in new Westminster police hybrid patrol car fleet

Behind the Badge

The Westminster Police Department patrol vehicle fleet is going greener. In the coming weeks, the department is set to receive its first hybrid car, a U.S.-made 2021 Ford Explorer. The car will be one of nine within Westminster's fleet. The department is leasing them to provide some short-term savings over buying.

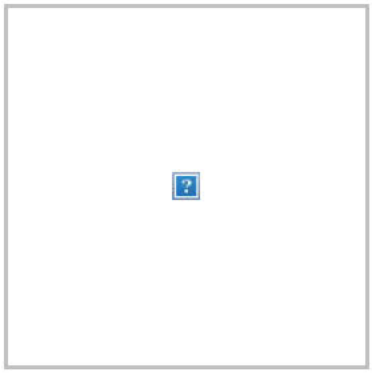
READ MORE

Los Banos police to install license plate readers in city. Here's how they work

Merced Sun-Star

Los Banos may soon receive a new technological set of tools to help solve crimes and look out for suspicious vehicles. The city's police department gave a presentation to the City Council last week about its plans to use Automated License Plate Readers (ALPR) in the city. The ALPR technology reads license plates as drivers pass through the city. As a result, officers say they are provided with information that can help with criminal investigations.

READ MORE



Union-Made backyard BBQ

Union Plus

Fire up the grill for summer! We've got a line up of the best union-made/packaged hot dogs, beef, beer, grilling tools and recipes to make your next BBQ the best ever! No backyard? No problem! Set up the grill on your patio, balcony, courtyard or driveway. Happy grilling!

READ MORE

This simple formula will show you if you're on track to buy a home or retire early

CNBC

If you have a big money goal in mind, such as buying a home or retiring early, you should have a solid understanding of where your money is going, including how much you're actually saving. An easy way to figure out how much of your money can go toward building wealth is by calculating your savings rate, which is the percentage of your income that you keep each month, versus the amount that you spend.

READ MORE

These mind games can help you save more money

MSN

Saving for your goals is important, but it's not always the most fun or interesting task. If you want to boost your bank account and start a savings habit that lasts, consider using money-saving challenges to shake things up. In this list, you'll find challenges and tools that can help you reach your savings goals, whether it's to pay for a dream trip or to save money for a big purchase.

READ MORE

IRS sending letters to more than 36 million families who may qualify for monthly Child Tax Credits; payments start July 15

Internal Revenue Service

The Internal Revenue Service has started sending letters to more than 36 million American families who, based on tax

returns filed with the agency, may be eligible to receive monthly Child Tax Credit payments starting in July. The expanded and newly-advanceable Child Tax Credit was authorized by the American Rescue Plan Act, enacted in March. The letters are going to families who may be eligible based on information they included in either their 2019 or 2020 federal income tax return or who used the Non-Filers tool on IRS.gov last year to register for an Economic Impact Payment.

READ MORE

5 key considerations as you craft your retirement plan

Kiplinger

Stashing away money for retirement is both smart and necessary to increase the odds that you will be financially secure once your working career comes to an end. But the act of saving money is not in itself a retirement plan. You also need to be intentional in establishing how much money you will need, when and how you will spend it, how taxes might affect you, and a host of other issues.

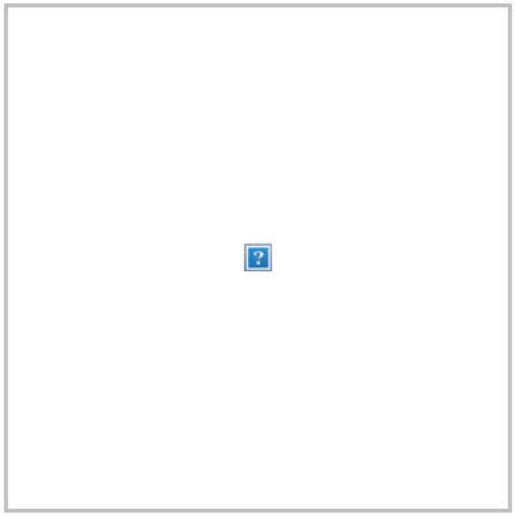
READ MORE

Stretch your dollar: Money-saving life hacks to keep you and your house cool this summer

WTNH

This week has many of us thinking about staying cool this summer! And while pools and beaches are nice. It's going to take more than that in the day-to-day. We are stretching your dollar with a few life hacks experts say can keep you cooler and, in some cases, save you money.

READ MORE



Heroes Vacation Club has 10 great tips for traveling with kids for I.U.P.A. members!

I.U.P.A. Briefing Room

Trying to decide what to do on your next vacation? We've rounded up some fun ideas to answer the who, what and where of how to travel next. When you're traveling with kids, any trip can feel l ke you're planning a mission to Mars. Whether you're traveling by land, sea or air, executing your travel plan takes forward thinking and precision to ensure a successful trip. When the kids are involved, organization is the key. At Heroes Vacation Club, we've come up some helpful tips to help make your next trip a success.

READ MORE

Card-reading device offers Westminster police helpful tool in ever-evolving 'slaphouse' investigations

Behind the Badge

Westminster Police Department's financial crimes/fraud detectives have a new device to add to their crime-fighting toolbox in their work against the ever-changing illegal gambling rings known as slaphouses. It's called the ERAD, which stands for Electronic Recovery and Access to Data. And what it can do is determine funds balances in any prepaid card with a magnetic stripe — gift cards, for example.

READ MORE

Milton Police receive grant to further de-escalation training

North Fulton Neighbor

The Milton Police Department has been awarded a $119,323 grant to offer officers simulated scenarios to bolster their de-escalation and defensive tactics knowledge, skillset and philosophy. The department is one of over 60 agencies statewide to receive these first-ever grants from the State of Georgia's Criminal Justice Coordinating Council. The funding, which must be used for use of force or de-escalation training, is available through June 30, 2022.

READ MORE

Freeport Police hope new ShotSpotter technology will improve response times to gunfire

Rockford Register Star

The Freeport Police Department hopes its $50,000 gunfire-detection system will help officers cut down on the time it takes to respond to shots fired. ShotSpotter, technology that uses information from multiple sensors to cross-check gunfire locations, is billed as more reliable than the human ear to identify gunfire. The technology was implemented in mid-May, and Freeport Chief of Police Matthew Summers says the system will be evaluated each year to determine whether it will continue to be used.

READ MORE

The New York City Police Foundation announces first 22 grant recipients of the '50 Grants for 50 Precincts' program

New York City Police Department

The New York City Police Foundation today announced the first 22 winners in its $1 million grant program to create innovative new projects at NYPD precincts. Among the winning innovations are those to promote engagement between police officers and kids, officer wellness, strengthen community engagement, honor fallen officers, and more.

READ MORE

DA Michael W. Morrissey awards $5K 'Mental Health First Aid' police training grant

WickedLocal.com

District Attorney Michael W. Morrissey recently awarded $5,000 grants to support mental health needs in 15 communities across Norfolk County, including Randolph. "We offered communities grants for three set programs or the flexibility to propose their own according to their needs — as Randolph chose to do," Morrissey said. "I have to commend Randolph Police Chief Anthony Marag for choosing to provide Mental Health First Aid training to 100% of his staff with this grant."

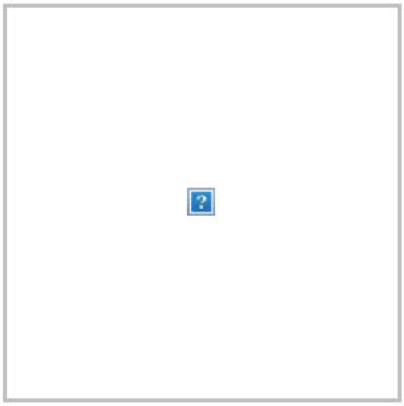
READ MORE

The early chronicles of Spot, the robot police dog

Government Technology

Police surveillance in the U.S. is a hot-button issue, thanks in part to the rise of drone technology among law enforcement during the pandemic last year. Just over a month ago, a robot dog, also known as Spot or “Digidog,” became part of the conversation about surveillance as the New York Police Department faced criticism for utilizing the machine.

READ MORE



Our diets may be more deadly than smoking

Humana

If you ask people what’s the one human behavior that causes the most deaths, chances are, many may say smoking. But as bad as smoking is, new research suggests that the food choices we make create an even larger health risk.

READ MORE

There's a very good chance you're not eating enough fruits and vegetables

Humana

Fruits and vegetables are important to good health, according to the Centers for Disease Control and Prevention, or CDC. Yet just 1 in 10 adults meets the federal recommendations for daily servings of fruit and vegetables, according to a CDC analysis of data from the 2015 Behavioral Risk Factor Surveillance System.

READ MORE

Does exercise help protect against severe COVID-19?

Harvard Health Publishing

Science shows us that being physically active helps us feel better, and prevents or slows many diseases, including heart disease, cancer, and dementia. It even helps us live longer. For these reasons, the US physical activity guidelines and the American Heart Association recommend at least 150 minutes of moderate physical activity weekly. Now, a study in the *British Journal of Sports Medicine* suggests that routine activity may help protect people who get COVID-19 from becoming seriously ill.

READ MORE

Doctor's advice on how to plan a safe summer during pandemic

NBC DFW

Parents are in midst of planning a big summer for their kids. With the help of the COVID-19 vaccines, the hope is to re-create summer memories they had before the virus, while also preparing them for life beyond the pandemic. NBC 5 spoke to a local doctor for insight on how parents can find some normalcy again at playgrounds, summer camps and family trips while also staying safe.

READ MORE

COVID-19: Healthy kids

Wisconsin Department of Health Services

Find guidance and resources for caring for Wisconsin children from the Wisconsin Department of Health Services.

READ MORE

Can exercise lower your cancer risk?

The Baton Rouge Clinic AMC

Here's some good news for active people. That daily walk, jog, fitness class or bike ride might be doing more good for your body than you realize, especially when it comes to cancer risk. A strong link has been shown between higher daily levels of physical activity and a lower risk for developing several types of cancer, including breast, colon, esophageal, bladder, kidney, stomach and endometrial, according to the National Cancer Institute (NCI).

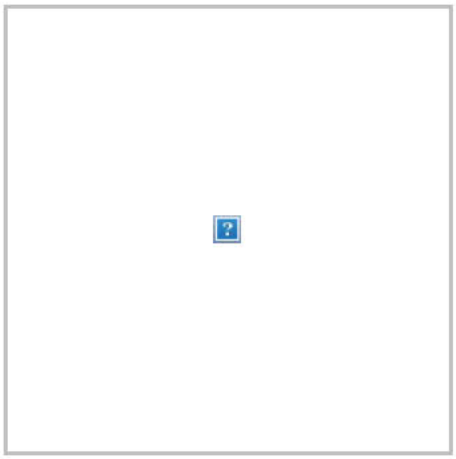
READ MORE

What's the point of exercise?

WGBH News

Exercise is a relatively recent phenomenon. After all, it's difficult to imagine a caveman on a treadmill. And it's safe to say that paleolithic humans never pumped iron. But something changed as we moved from the plow to the Peloton. Exercise — physical exertion for the purpose of improving health or fitness — became a huge part of modern life, and a nearly $100 billion global industry.

READ MORE



Police officer, passerby fold American flag after its knocked down during high wind

Officer.com

Caught on Camera: Police officer, passerby fold American Flag after its knocked down during high winds (video courtesy: Renew Community Church)

WATCH NOW

Somerville Police to escort Special Olympics torch down Main Street

TAP Into Somerville

A pack of Somerville police officers and civilian police dispatchers will take off from their staging point in front of the Van Derveer School to escort the Special Olympics Torch of Hope through the downtown shopping and restaurant district. Somerville Police will pick up where a group of Bridgewater police and Somerset County Sheriff's Officers left off after its escort through Bound Brook and Bridgewater.

READ MORE

Hidalgo County Sheriff's Office supports honorary deputy in cancer fight

ValleyCentral.com

The Hidalgo County Sheriff's Office showed support to a local boy battling cancer. The Hidalgo County Sheriff's Office pinned Adan Alejandro Farias with an honorary deputy badge, over the weekend. Sheriff J.E. "Eddie" Guerra and his staff welcomed Farias to the Hidalgo County Sheriff's Office family.

READ MORE

Holly Springs Police Department holds fundraiser to help retired officer in need of double lung transplant

WNCT News

he Holly Springs Police Department and the community came together Saturday to help raise money for a retired sergeant who is in need of a double lung transplant. Sgt. Rick Leach served the Holly Springs community for over 25 years as a police officer, school resource officer and a sergeant over the SRO division. He was diagnosed with pulmonary fibrosis and will need a double lung transplant to save his life.

READ MORE

Therapy dogs, new pup, bring relief for police, community

Officer.com

Three of the most popular members of the Albany Police Department are in serious need of a shave. Meet the triumvirate of Maxie, Finn and a third friend still to be named — police dogs whose talents involve sloppy kisses more than sleuthing for clues. Maxie, 3, a female Black Labrador donated from a breeder in the Mohawk Valley, and Finn, 4, a male black Labrador rescue from Brevard County, Fla., are existing therapy dogs for the capital city's force.

READ MORE

Photo of the Week: Twilight traffic

Police 1

This week's photo comes from Jeremiah Erickson of the Camp Ripley Department of Public Safety in Minnesota. Erickson, who also manages his own photography business, took this shot of a train at sunset while managing traffic. Officers need to block traffic to allow the trains to move safely through a busy section of highway, Erickson said.

READ MORE

IUPA E-Trends

Connect with IUPA

Jason Zimmerman, Director of Publishing, Multiview, 469-420-2686 | Download media kit
Robbie Vaglio, Content Editor, Multiview, 469-420,2625 | **Contribute news**

International Union of Police Associations
5632 Bee Ridge Road, Suite 200 | Sarasota, FL 34233
800-247-4872 | Contact Us | www.iupa.org

Click here to unsubscribe.

Learn how to add us to your safe sender list so our emails get to your inbox.

ASSN PNG LOGO

ADVERTISE

SUBSCRIBE

PAST ISSUES

7701 Las Colinas Ridge, Ste. 800, Irving, TX 75063

From: The Axon Team
To: McCarthy, Steven (POL)
Subject: Here"s your chance...ask us anything about Fleet 3!
Date: Friday, June 25, 2021 1:07:32 PM

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

Axon

Fleet 3 is hitting the road, and we want to know what you want to know.

Join Rick Smith, Chief Executive Officer, Jeff Kunins, Chief Product Officer, and Blake Bullock, Director of Fleet Products, for an Ask Me Anything-style webinar about our next-generation in-car camera system.

Curious about our integrated ALPR? Want to learn more about our Respond real-time alerts and streaming? Want to see how Fleet 3 can make your agency more efficient and collect better footage?

REGISTER NOW

We can't wait to hear from you!

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe





From: International Association of Auto Theft Investigators
To: Atkinson, Dana (POL)
Subject: IAATI - Member Update
Date: Tuesday, July 20, 2021 6:07:46 PM

19th July 2021

View this email in your browser

Hi Dana,

69th International Conference just 3 weeks away

Thought you had missed out on participating in the 69th Annual Training Seminar because of travel restrictions, finances or work pressures?

Then we have the way you can still be a part of this major event. See the first article below on how IAATI is using technology to enable all members to participate, no matter where they are based.

Also in this issue of *Member Update*:

- **NERC's July's free webinar** hosted by Carfax is on the really interesting topic of the use of drones in law enforcement and insurance applications, developing a drone program, and best practices to prevent bad case law. This webinar is open to any IAATI member so please read the article below and register for the webinar.

- **SERC's free webinar** on 'Auto Theft Trends" is scheduled for 1.00 pm (EST) on August 3rd, 2021. Please see the article below for details and how to register.

- **July is Auto Theft Prevention Month**. Have you helped spread our *No Regrets - Lock it, or Lose it* campaign message? If not, please read the article below, so we can all help raise awareness of the problem of vehicle related crime and how the simple act of locking your vehicle and removing your keys is the first step we should all be taking to help reduce vehicle theft. We also ask that you share the prepared resources with your employer and get them lend their support by circulating the material. They are even welcome to include their logo alongside IAATI's on any of our digital images.

- Don't forget you can order your 2021 Conference merchandise and have it delivered to your home or pick it up at the conference (see below for more details)

- All the details about how you can attend our **Annual General Meeting (AGM)** either in-person or virtually via Zoom.

Just on the last point about our AGM. IAATI is your Association, and as such our **Annual General Meeting** is extremely important. It is your opportunity to learn more about what is happening on the Board and its numerous committees; a chance to vote for any changes to our Constitution; to vote for our next team of Board members; as well as provide feedback or ask questions of the Board. This year all members have the opportunity of participating and voting in the 2021 AGM no mater where you are in the world. All we ask is that you register you interest in attending the AGM so we can ensure we have enough capacity in our Zoom license. Pre-registration is requested for both members who will be attending the meeting in-person in Denver or on-line. For those members who have registered, you will receive an email with the full set of agenda papers seven days prior to the meeting, along with instructions of how to log-in to meeting. See the article below for more information, including how to register your interest in attending the AGM.

I encourage you to to read the following articles and I particularly encourage you to take up the special offer to join us remotely for our 2021 International Seminar.

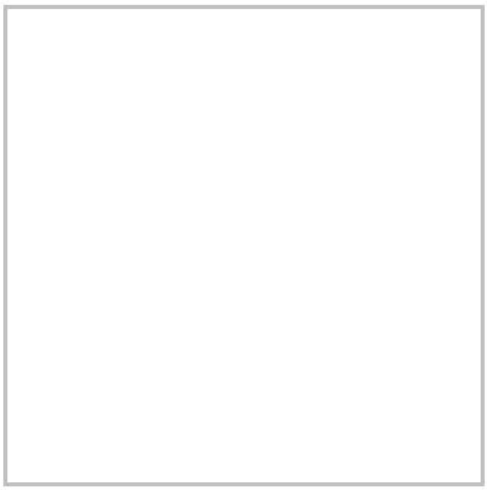
Finally wish would like to send a special message of support to our IAATI family and friends in South Africa who are experiencing some troubling times. We are praying for you and your families.

Take care and stay safe.

Paul Thomas
1st Vice President

Think you can't attend the 69th International Conference in Denver next month?

Yes you can! Just $US50 as an on-line delegate.



Yes that is right, even if travel restrictions, finances or work commitments are preventing you from attending our 69th International Conference in-person, you can still view the majority of the classes via a live-stream or recording.

For just $US 50 members can register as a 'remote' delegate. As such you will be able to:
a) connect and view the vast majority of activities on-line, and
b) view recordings of the vast majority of the classes for a limited time after the conference.

So for less than the cost of a taxi fare to the airport you can sit at home or in your office and learn new information to be more efficient in you daily job.

Register now at https://iaatidenver2021.com/registration/

While we all agree nothing beats being at the annual International conference in-person, but this is the next best thing. Now, no matter whether you are based in USA or anywhere else in the world, you can still be a part of IAATI's premier training event of the year, and keep up-to-date with the latest trends and issues from our hand picked range of international experts.

But I live in a different time zone. No problem, you to can watch the class live in your time zone, and if this means they are scheduled in the middle of the night for you, then you may prefer to watch the recordings at your leisure. You can even do both - watch classes live and then watch recording of other classes or even review some of your favorite classes multiple times.

One of the of the highlights of this year's conference is sure to be a class on the best practices for conducting online searches and intelligence gathering. Searching online for open source intelligence (OSINT) has become a true art nowadays, and time consuming. Things are running great and then suddenly, Facebook makes major changes and you can't find what you want anymore. You are tired of looking at a million plus Google results, and you aren't sure what platform you should be searching anyway. Worse, you aren't sure what to do after you find that critical evidence.

To cover this topic we have leading international expert Joe Stephenson from Intertel inc. Joe's

class will help you navigate through the online research process by reviewing some of the best techniques (and fastest ways) to uncover information online and how to best secure it once you have it. From using refined Boolean searches on Google, Twitter and yes, even Facebook to incorporating mobile devices in your process. More importantly, he will discuss creating a solid digital chain of evidence. Recent US case law throwing out screen-shots because they could not be authenticated now dictates your need to not only capture and validate the data but ensure that you can recreate it during future litigation.

Joe's classes are always fun and informative and this class alone will be worth more than the $50 remote registration fee.

But this is just one of many classes each day. Don't miss out on learning:

- How Police in Australia are using their award winning VIPER Platform to integrate a range of video and camera data to transform the vehicle identification process and help solve hundreds of crimes from homicides, abductions to armed robberies and being adopted within the policing COVID 19 response.

- An in-depth look at altered and fictitious documents used by today's sophisticated auto thieves to steal vehicles and attempt to lend legitimacy to the stolen vehicle after it's theft so that it can be operated openly or sold for large profit. A look at how to detect these documents and the hurdles presented in combating and preventing these crimes.

- Hi Tech Tips & Tricks for the Investigator. This class is a presentation on the new Con's, Scams and Crimes that are happening and are soon to be here. This class will show, explain and demonstrate new techniques, tools and resources for Law Enforcement and corporations. This includes tools that are commercial and free. It cover Frauds, Forensics, Online investigations, financial crimes, Officer and personal safety as well the Dark and Undernet.

- Multiple classes on all the latest in the field of digital vehicle forensics.

- VIN Reconstruction as an investigative technique that can be used to identify suspect vehicles from images and videos, generating a viable list of filtered leads in criminal cases.

- The dynamics of plant and agricultural and heavy machinery theft.

- Understanding tell tell signs of non-criminal behavior vs. criminal behavior within Mexican Cartels & Narco Culture

- A understanding of Keyless Ignition Systems in a course specially designed for insurance fraud investigators, licensed adjusters, case managers, and claims professionals whose duties require them to investigate questionable claims.

- and so much more for

To see the full conference program visit: https://iaatidenver2021.com/agenda/

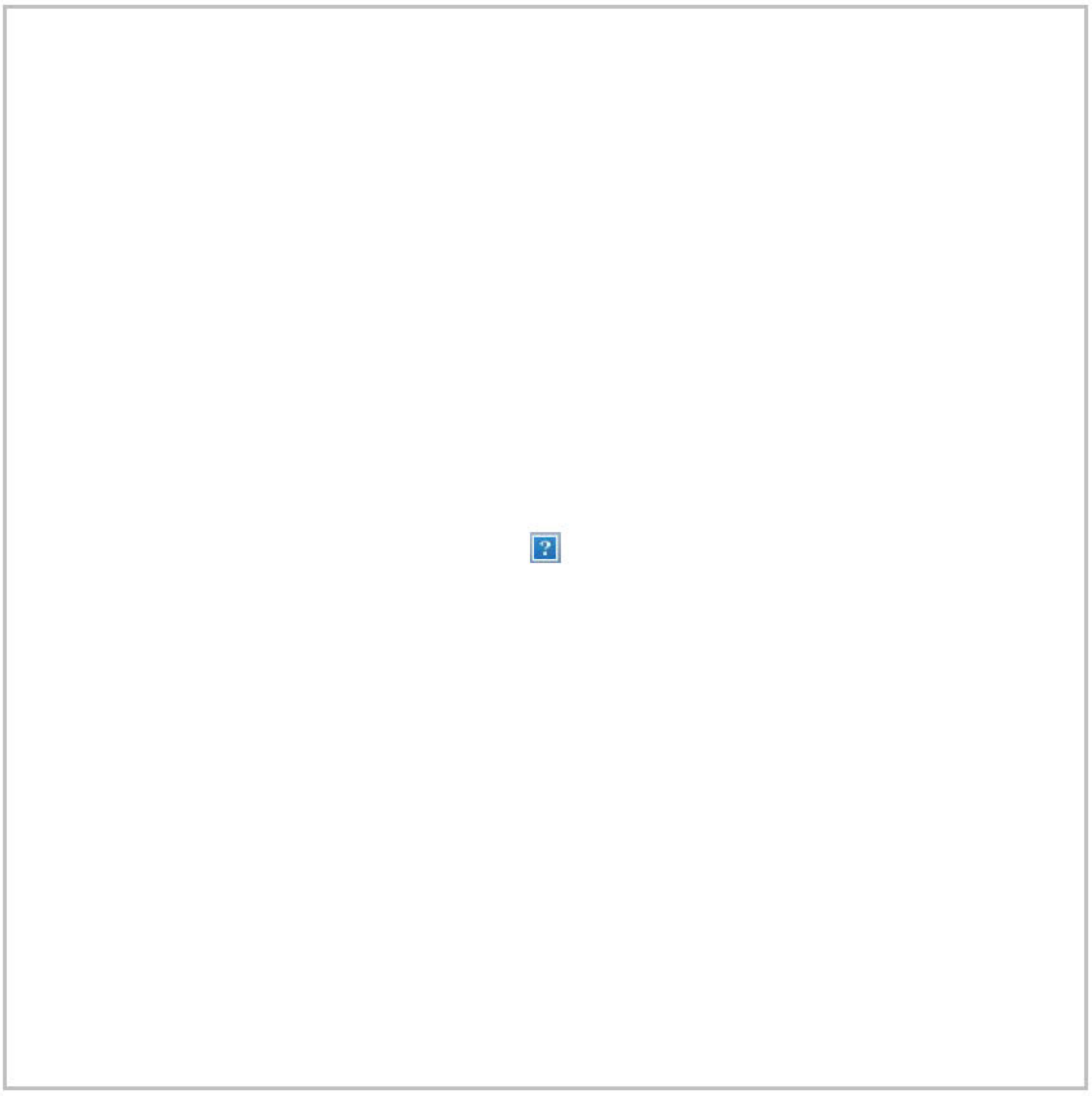
Register now as a remote delegate
To take advantage of this incredible $US 50 remote registration offer, and learn more in week than you can in a whole year, click: https://iaatidenver2021.com/registration/

Attending in-person?
If you re attending in person then you too will also get access to the recordings after the conference so you will be able to view classes you couldn't attend or review some of your favorite classes.

We currently have over 400 people registered to attend the Conference in-person, so this is clearly going provide a great networking opportunity if you can get to Denver.

Also for those delegates in Denver, don't forget to check out and visit the various sponsors and vendors who are supporting the Conference. These include:

- Diamond Sponsors:
  - Leonardo /ELSAG ALPR Solutions
  - Planet Technologies Inc
- Gold Sponsors:
  - Berla
  - GM / Onstar
- Bronze Sponsor:
  - Neology
- Newsletter Sponsors:
  - Assisted Patrol
- Vendors:
  - CovertTrack Group, Inc.
  - CRIMEWATCH Tech, Inc.
  - Flock Safety
  - Motorola Solutions Inc / Callyo
  - Point Blank Enterprises



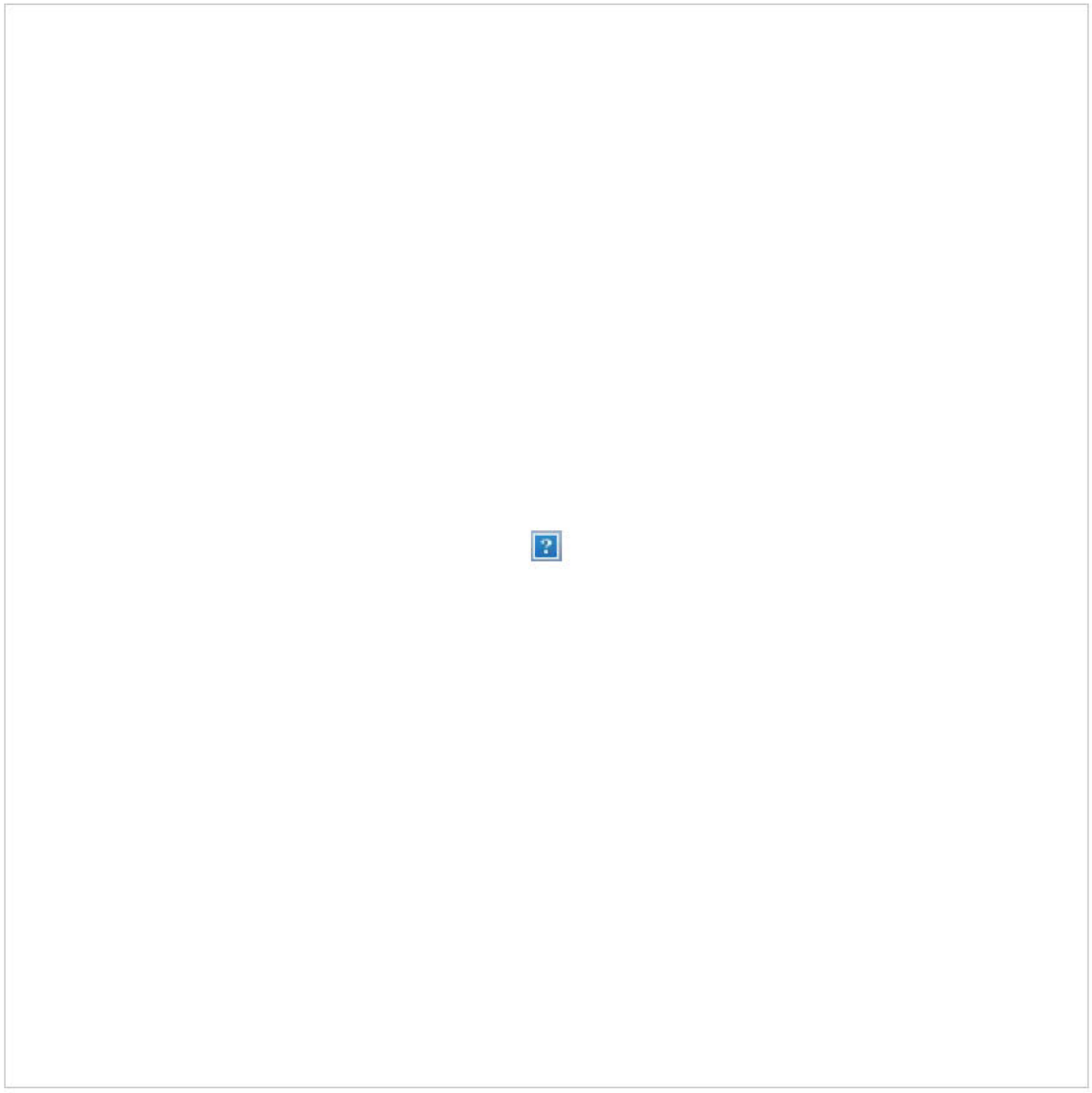
NERC Free Webinar - July 29th

The next free webinar presented by NE-IAATI is scheduled for July 29, 2021, at 1:00 p.m. (eastern time) and will cover unmanned aircraft, specifically, the use of drones in law enforcement and insurance applications, developing a drone program, and best practices to prevent bad case law. This block is presented by retired New Jersey State Police Sergeant First Class Ron Leach. Mr. Leach is the principal of Leach Strategic Partners and holds many FAA pilot certifications and aircraft qualifications. He spent more than 15 years in the NJSP Aviation Bureau where he served as a Captain of all NJSP aircraft and flew all mission profiles. Mr. Leach has been published in NJ Cops magazine, presented to the New Jersey State Association of Chiefs of Police, and contributed to the ANSI UASSC Standardization Roadmap for Unmanned Aircraft Systems.

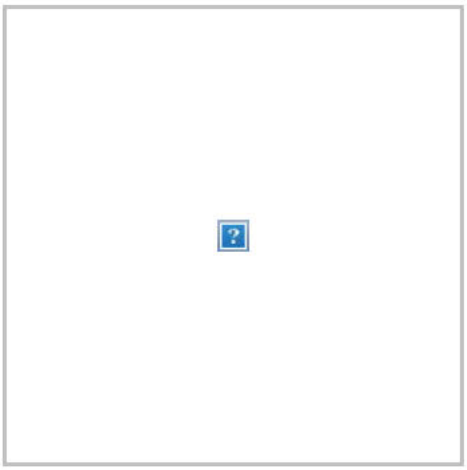
This seminar is open to any IAATI member, anywhere in the world.

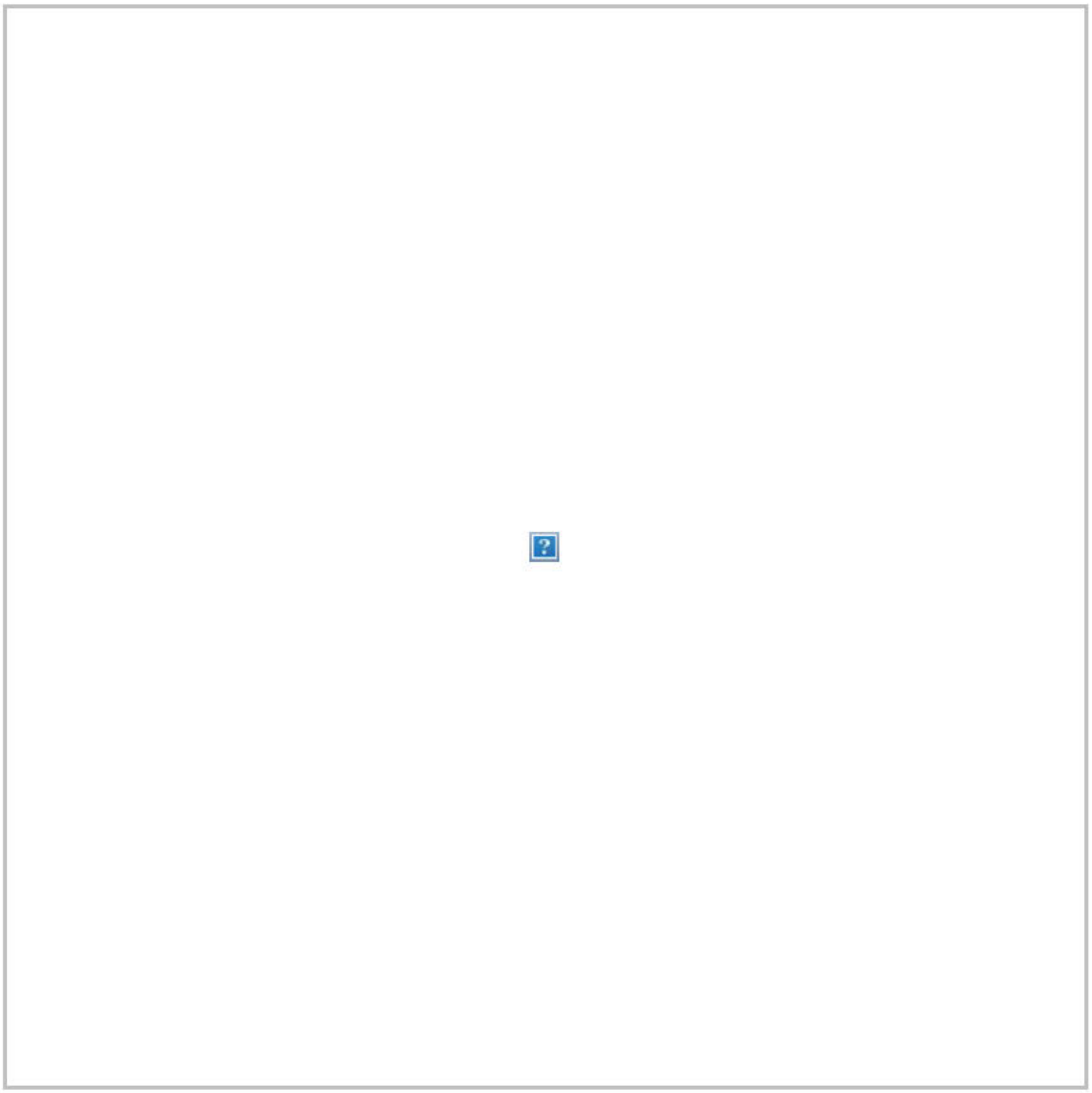
Register for the webinar here: https://content.carfax.com/NEIAATIJuly21LP.html

If you have any questions reach out to Cory Rodriguez at CoryRodriguez@gmail.com or Michael Ledoux at MichaelLedoux@carfax.com.



SERC Free Webinar - August 3rd





Carfax for police will be offering virtual training for SEIAATI Members on August 3, 2021 at 1:00PM (EST). To register for the training, please follow the link and complete the registration form. Thank you to Carfax for providing this training to our members!

The registration form can be found here:

https://content.carfax.com/2021-08SEIATTI-LP.html

Attend our Annual General Meeting from anywhere in the world

President Tinus Odendal is pleased to invite all current members of the International Association of Auto Theft Investigators to attend the Annual General Meeting, which is being held both virtually and in person on Thursday, August 12, 2021 from 08:00am to 10:00am Mountain Time.

The Annual General Meeting will be held at the Omni Interlocken Hotel, 500 Interlocken Boulevard, Broomfield, Colorado (USA) 80021, in the Interlocken Room.

Please be advised that any and all motions or votes requiring a count will be conducted electronically using the polling feature in the video conferencing software.

Registering for the Annual General Meeting:

ALL MEMBERS who wish to attend the AGM, either in person or virtually are asked to register for the AGM via the link below. This is a separate registration process for the Conference registration and there is no cost to attend the AGM.

Even if you are attending the 69th Conference in-person, you are still asked to register for the AGM by 30th July 2021 using the ink below so we can cater for the expected number of members.

To Register visit: https://www.iaati.org/events/entry/2021-annual-general-meeting

This year all members participating in the AGM (whether present in-person or attending virtually) will be required to bring a smart phone / computer / tablet with internet access in order to vote in any motion or the elections. WI-FI access will be provided to those members attending the meeting in person. You are strongly encouraged to ensure that your Zoom software has been updated to the latest version so you can vote in the online polls.

By registering your intention to attend the AGM you will:

- help us plan the room size and our video conferencing license size
- allow us to email you, one week prior to the meeting:
    - the meeting link and password
    - the AGM Agenda and Committee reports, so you can read them and make informed decisions before voting
    - instructions on how to cast your votes during the meeting
    - instructions on testing you have the correct versions of the conferencing software

on your phone, laptop or tablet..

Correction: In previous emails about the AGM it was stated that unless you register your intention to attend the AGM by the 30th July, you will not be able to attend the AGM and vote. This was incorrect. If you don't pre-register you may still be able to attend but if large numbers of members decide to try and attend on the day without pre-registering, we cannot guarantee that we will have the capacity to allow you to vote at the meeting. Therefore, if you think you you may wish to attend, please help us out and RSVP by 30th July using the above link.

It is very important that members attend the AGM. This is your Association, and we need your feedback and direction for what you want from your Association. Over the last 18 months the Board has worked hard to ensure that we are even more transparent and treat all members equally. As a result there are number of changes this year to the AGM's Standard Operating Procedures, as well as changes to our Standard Operating Procedures and most importantly proposed changes to our Constitution.

The first of these changes to the Constitution is an amendment to allow all current members, no matter where they are based, to participate and vote at the AGM. Currently, those members who due to work commitments, finances, travel constraints, etc can not attend the AGM in-person, are unable to have their say and vote on the election of board members, or any proposed motions. This proposed amendment, if passed, will ensure every member has the same rights and equal opportunity to vote at AGMs. (Note this amendment will be discussed as the first item at the 2021 AGM, and if passed, will then enable the online members to vote in the remainder of the meeting.)

Secondly, the Board has agreed to publishing all AGM agenda papers and reports in advance of the AGM. This means that members can read each of the committee's reports, including the financial reports, Nominating Committee's recommendations, etc. and have time to consider them well in advance of the AGM.

Thirdly, we are inviting members to submit any questions to the board either before the meeting or during the meeting.

Fourthly, we have given a commitment that if there is insufficient time to answer all questions during the meeting (i.e. both submitted questions and questions raised from the floor of the meeting), any unanswered questions will be answered after the conference.

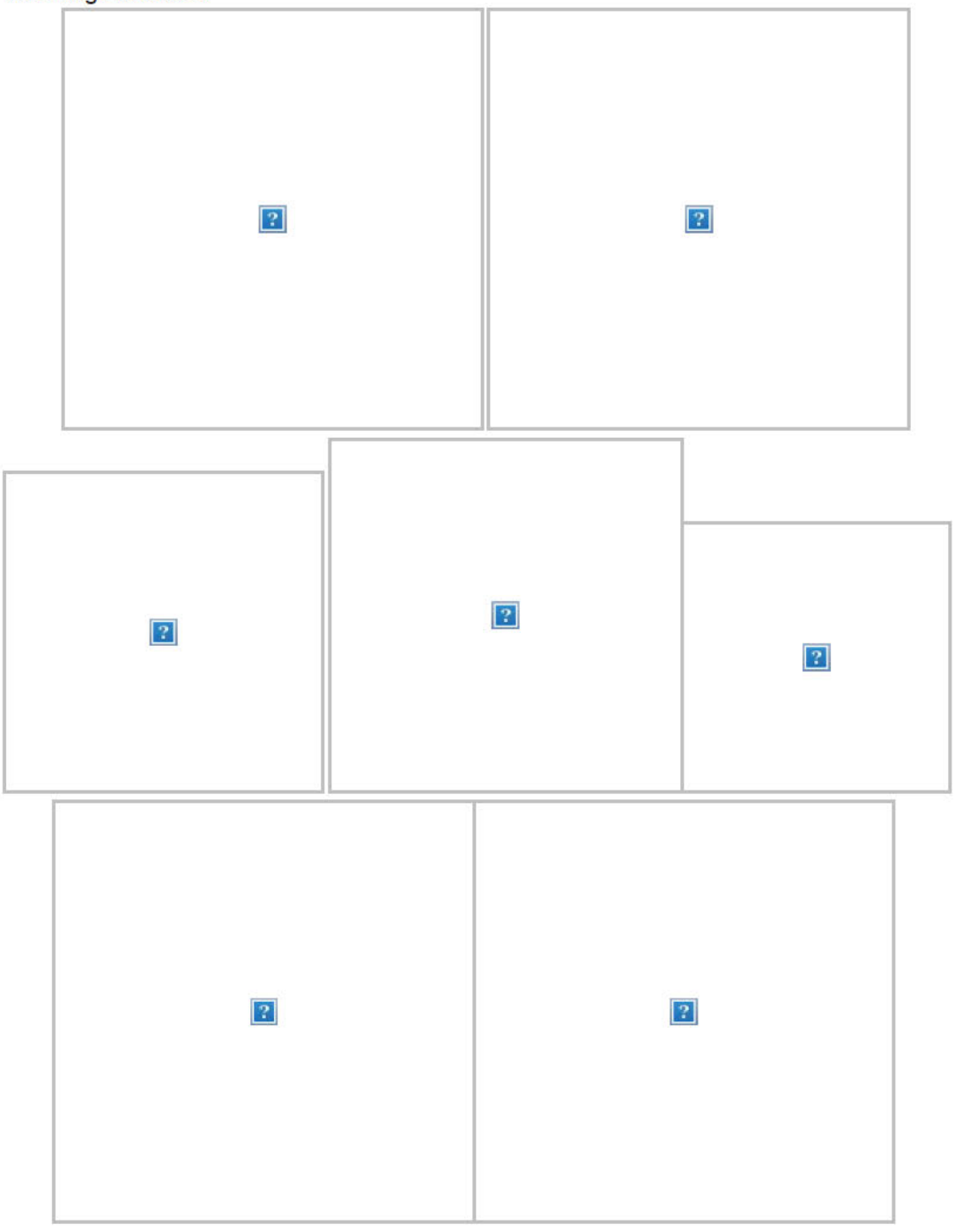
In summary, this year more than any previous year, all members can choose to participate in the AGM and have greater access to information. Please support the board and take advantage of these changes by attending the 2021 AGM either in-person or virtually.

Purchase your 69th Seminar Merchandise

No matter if you are attending the 69th International Seminar in-person or not, you don't need to

miss out on ordering your seminar merchandise to add to your collection. You can go online now and order from a range of products and collect them at the conference or have them delivered to your home.

The range includes:



To order merchandise visit: https://protect-au.mimecast.com/s/XyYqCjZrrnsjzMJvsWDqLs?domain=sparkmarketing.commonsku.com

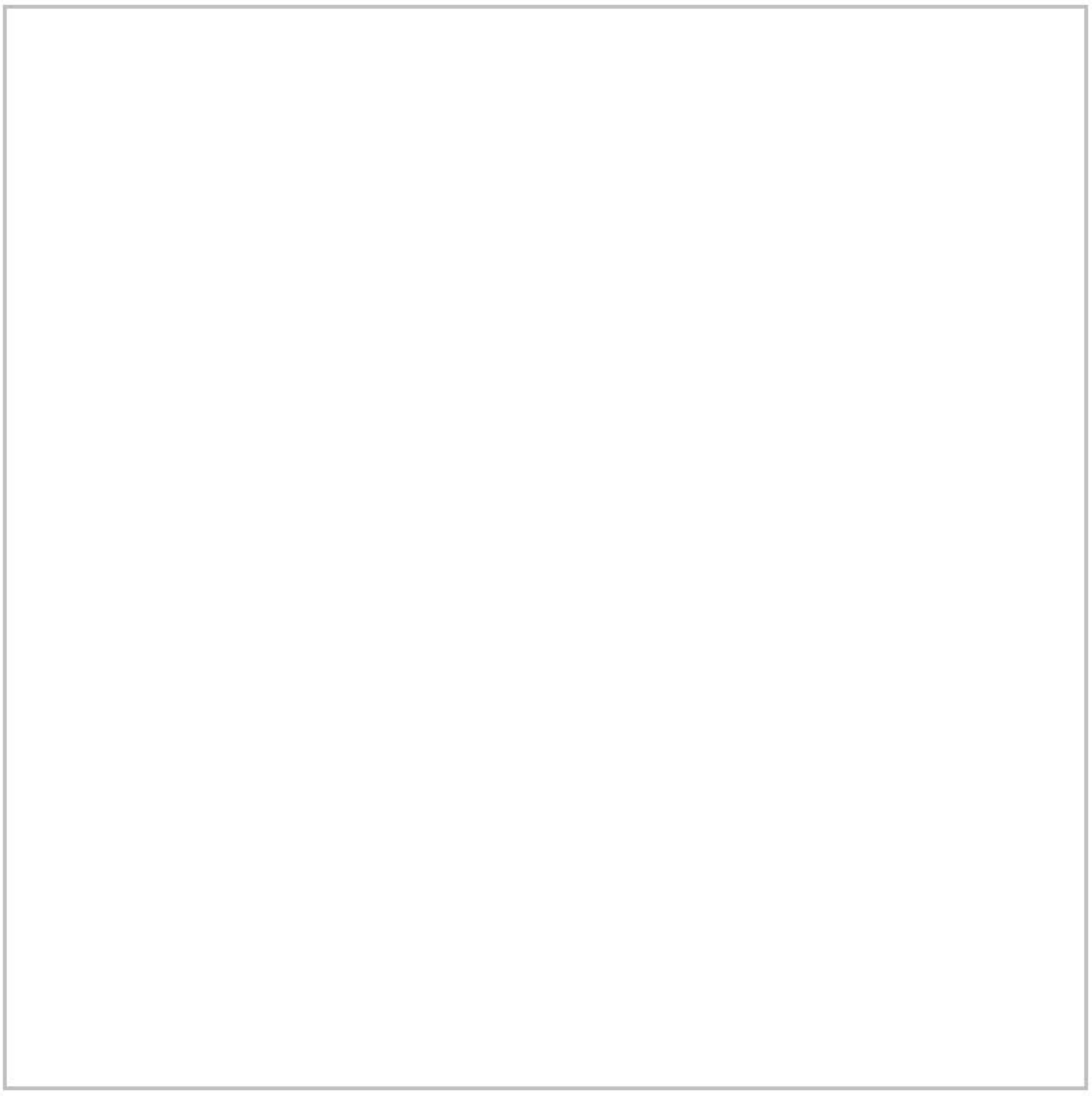
No Regrets - Lock it or Lose it

The month of July marks National Vehicle Theft Prevention Month in the United States. The International Association of Auto Theft Investigators (IAATI) and corporate partners located throughout the world are committed to increasing awareness and prevention of vehicle crimes while promoting proactive measures to protect vehicles from theft and burglary.

IAATI law enforcement and insurance members report most vehicle thefts are crimes of opportunity and therefore preventable. Simple steps taken by owners and drivers can help to reduce these crimes of opportunity. These steps include:

- Locking vehicle doors and remembering to close all windows and sunroofs
- Removing keys, and spare keys, from your vehicle
- Parking in a garage or behind a locked gate in well-lit areas whenever possible
- Removing any documentation that could be used to steal your identity
- Removing all guns and weapons from a parked vehicle
- Using additional security devices to assist in safeguarding vehicles from theft
- Safeguarding your car keys at all times
- NEVER leave a vehicle running while unattended

When everyone does their part to combat vehicle theft there are ***No Regrets to Lock it or Lose it.***



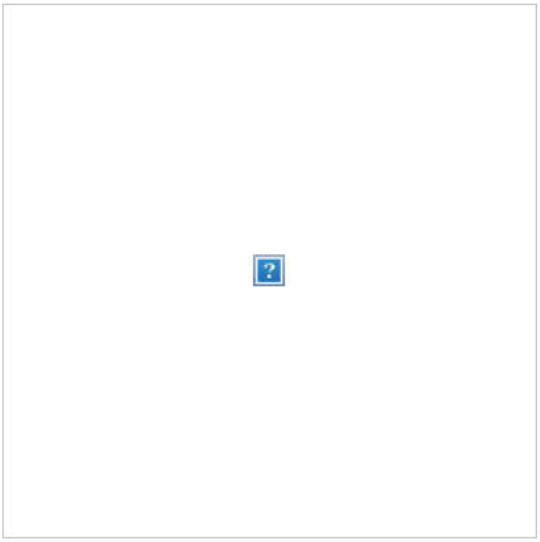
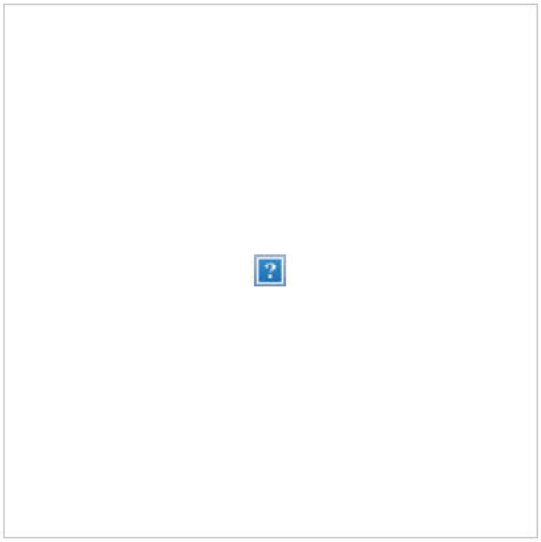
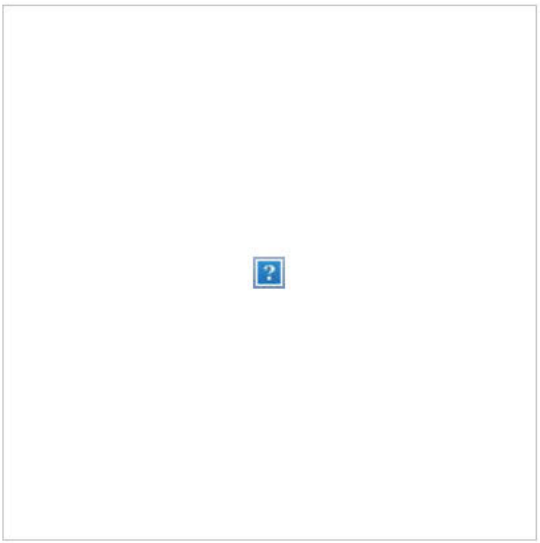
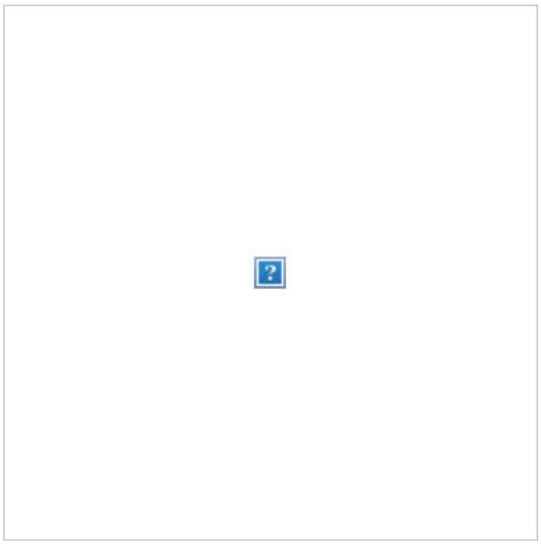
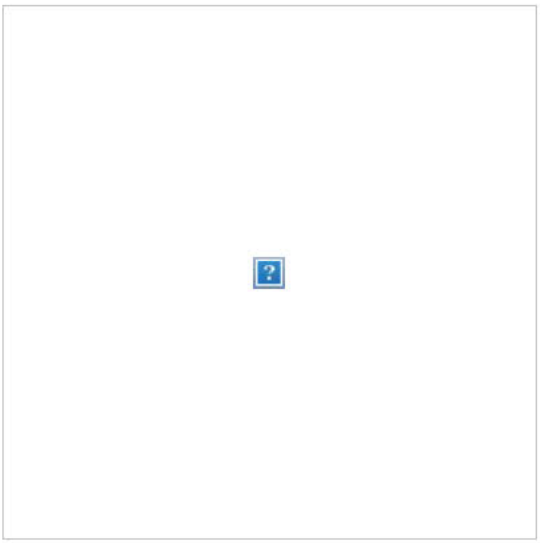
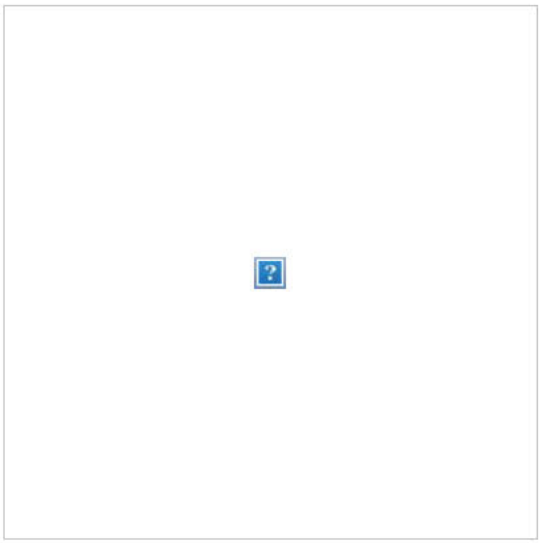
Thanks to the extremely hard work of Amanda O'Halloran and her Public Outreach Committee, they have prepared a range of material, such as verbiage for a state proclamation submission, a sample press release, and several media files that your agency can use on the various social media platforms (Facebook Twitter, Instagram and Linkedin).

IAATI is encouraging it members and their agencies all around the world to use our materials during the month of July and add their agency/company logo along side the IAATI logo. You can include them on your company websites, publications, social media sites and as part of your email signature block or in your own organization's media releases. By working together we add weight this important community message.

Feel free to use one, two, or all of adverts as you join us in the ***No Regrets - Lock it or Lose it*** campaign.

To download and use any of the free No Regrets - Lock it or Lose it campaign visit:

https://iaati.org/noregrets

This is the first of a number of campaigns that the Public Outreach Committee is aiming to develop. If you would like more information about this committee or want be involved in shaping and developing our future campaigns then please contact Amanda O'Halloran at Amanda.OHalloran@difi.az.gov

---

APB and Vehicle Crimes Today - our two publications

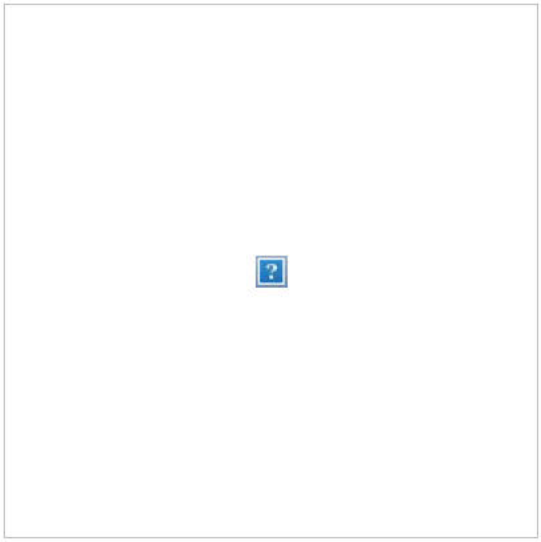
If you have read our July issue of *APB* I am sure you will agree it continues to be packed with a range of interesting articles. I challenge any member to not find multiple articles of interest in this issue.

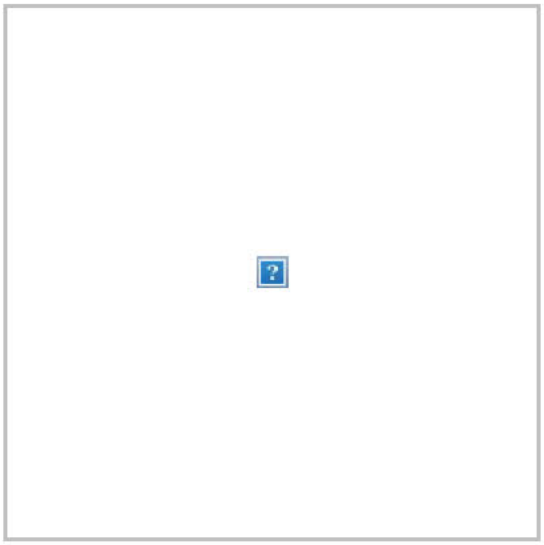
If you haven't read it yet, you can download and read it from our Resources menu on our website, but you must be logged in to the member only section to access it https://www.iaati.org/resources/publications

Similarly our monthly *Vehicle Crimes Today* (*VCT*) publication is always a source of information. *APB* is publish three times a year and *VCT* is published in each of the remaining 9 months each year. These publications require a lot of work and rely heavily on member contributions. So if you have a case study, an interesting article, photographs or video, an observation, comment or question you would like to pose to your colleagues, or even some social news about what is happening in your area, then please share them with your fellow IAATI members.

To submit content for publication in *APB* please email *APB* editor, Alex Lyle at alyle@cityofchesapeake.net

To submit content for publication in *VCT* please email *VCT* Editor, Nathan McGanty at nmcganty@gmail.com





Advertise in Vehicle Crimes Today

Vehicle Crime Today also accepts advertising and is a great way to get to message across to thousands of members around the world.

All adverts are full page size (US Letter) and the Advertiser is responsible for providing final publication ready artwork in electronic format. The deadline for all artwork and copy is 25th of the month prior to publication.

The rates for advertising in *VCT are*:

A full page advert in a single issue:	$US 200
A full page advert in two issues:	$US 350
A full page advert in three issues:	$US 450
A full page advert in 4 or more issues:	$US 125 per issue (minimum of $500 or 4 issues)

*Banner on vehiclecrimes.org website add $50 per package

To download the VCT Advertising Contract please click: https://www.vehiclecrimes.org/documents/AdvertisingContractVCT.pdf

This email was sent to dana.atkinson@pol.state.ma.us
why did I get this? unsubscribe from this list update subscription preferences
IAATI · PO Box 223 · Clinton, NY 13323-0223 · USA

From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: ITS America picks Laura Chace as new president and CEO
Date: Thursday, August 19, 2021 8:55:54 AM

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

News from Traffic Technology International View this email online

Podcast Events Videos

ITS America picks Laura Chace as

new president and CEO

The Intelligent Transportation Society's (ITS America) Board of Directors has unanimously elected Laura Chace as president and CEO, effective August 30, 2021. Chace, who currently serves as the association's chief operating officer, has been with ITS America since 2015 in increasingly responsible roles and brings 15 years of association management to her new position.



READ MORE



Statement concerning NHTSA investigation of Tesla crashes

The Advocates for Highway and Auto Safety (Advocates) have released a statement on behalf of the organization's president, Cathy Chase, addressing the Traffic Safety Administration (NHTSA) Investigation of crashes involving Tesla vehicles.

READ MORE



Project Endeavour offers AV passenger rides in London

Project Endeavour will conclude its multi-city demonstration of autonomous vehicle (AV) services with a final on-road trial in Greenwich, London this month.

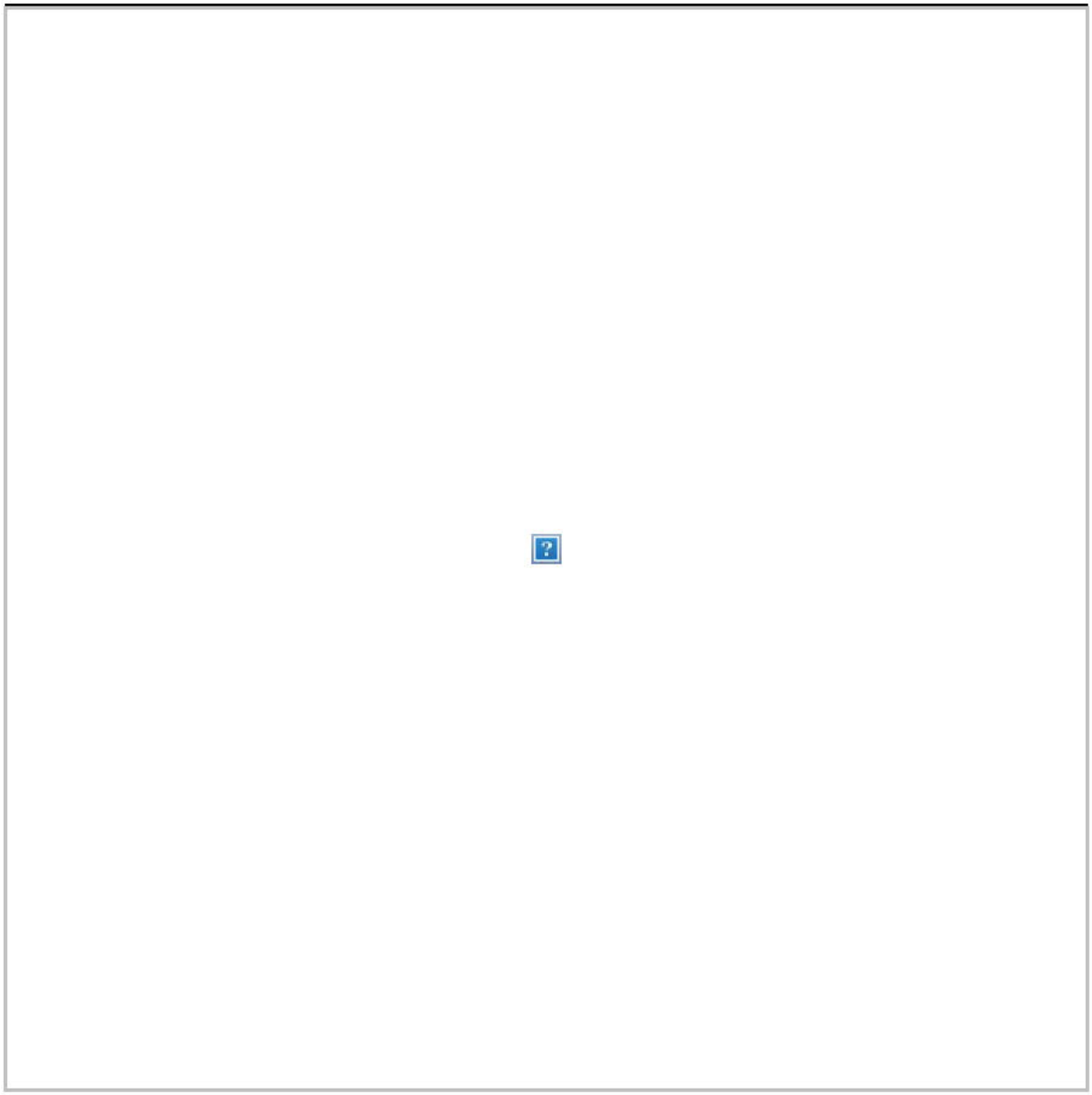
READ MORE

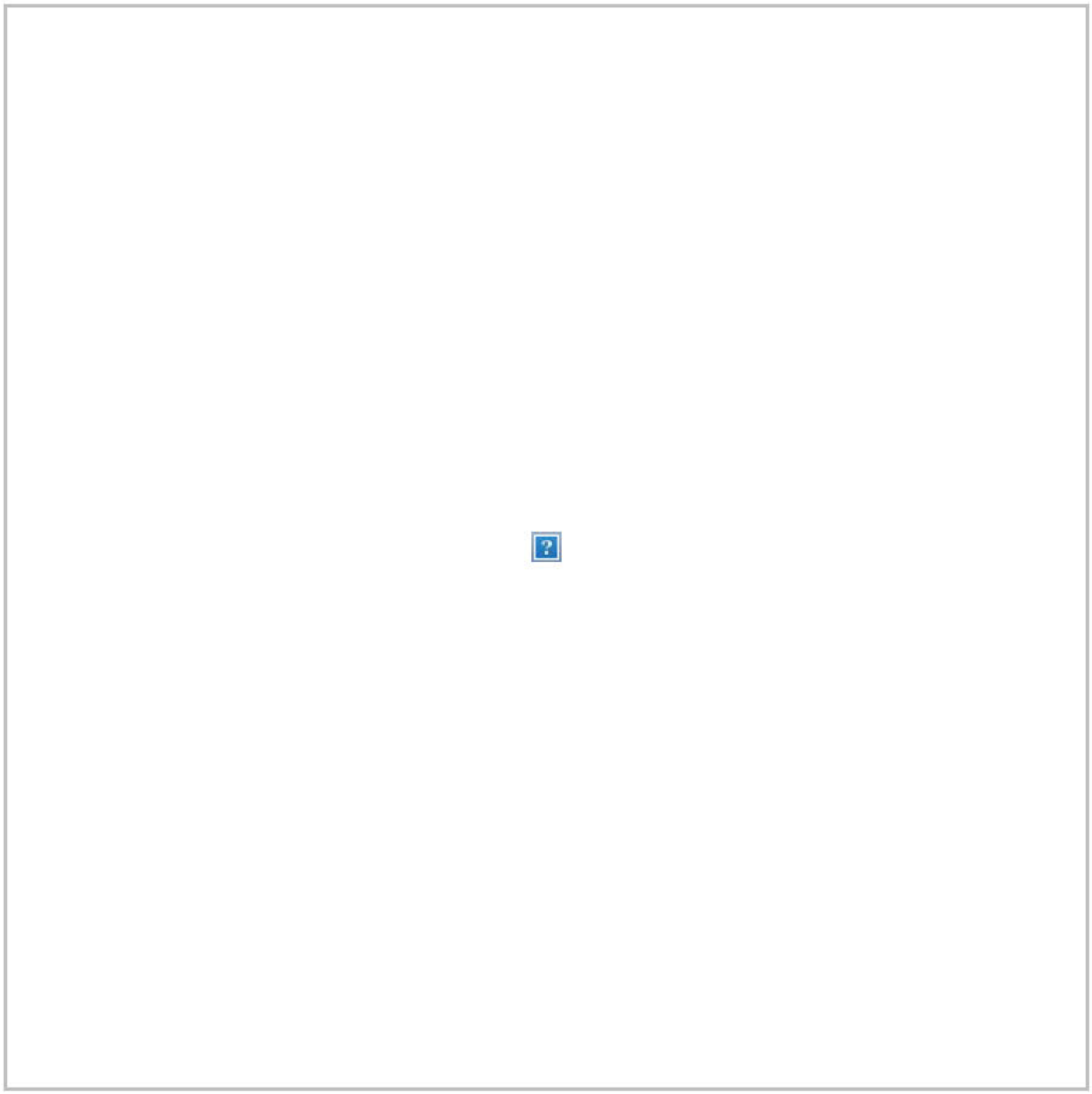
Vivacity Labs and TfGM to deploy cycling and walking sensors



Transport for Greater Manchester (TfGM) is set to advance its cycling and walking infrastructure programme through the rollout of new technology by Vivacity Labs.

READ MORE







May Mobility launches new on-demand AV shuttle in Michigan

May Mobility, an innovative autonomous vehicle (AV) technology and shuttle operations company, has announced the launch of an on-demand AV shuttle service in Grand Rapids, Michigan.

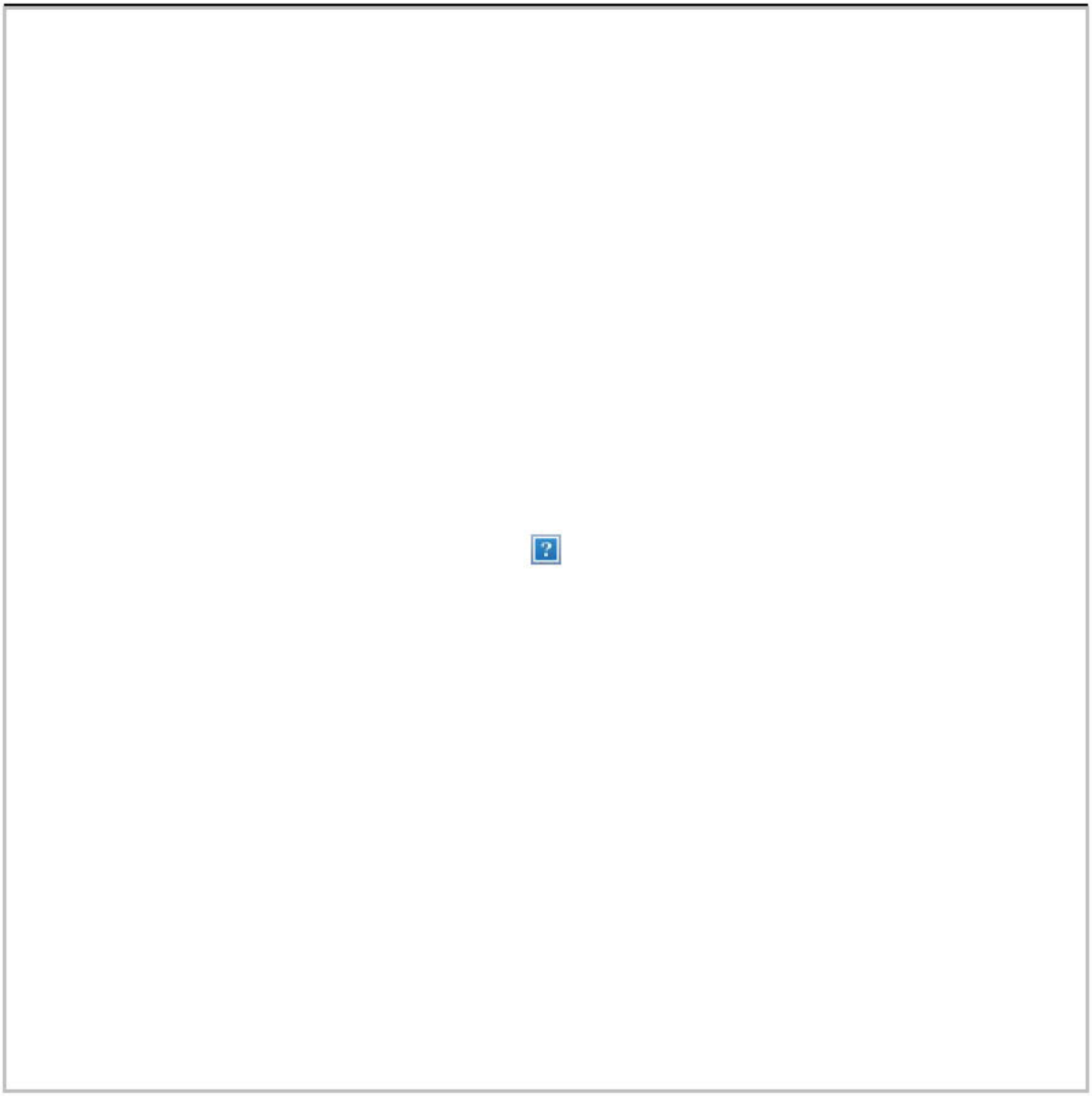
READ MORE

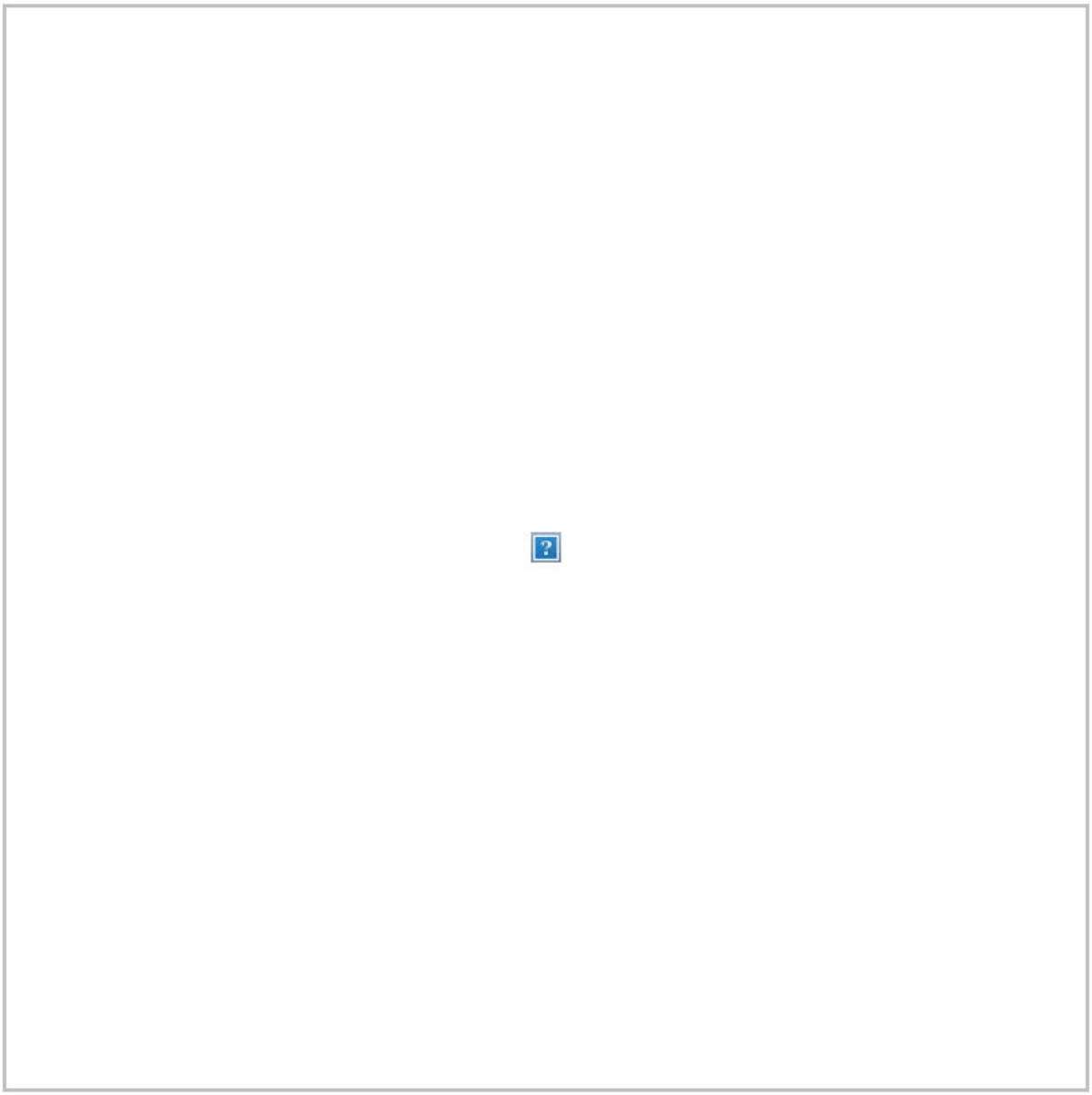


HERE research highlights connected car security fears

New research from HERE Technologies shows just one in five Australians feel comfortable with the cybersecurity and privacy aspects of connected cars. It also shows that discomfort accelerates with age.

READ MORE







New dataset will help AVs operate safely in bad weather

Sensors that operate in Scotland's rain, snow and fog are providing data that could help autonomous vehicles see and operate safely in adverse weather.

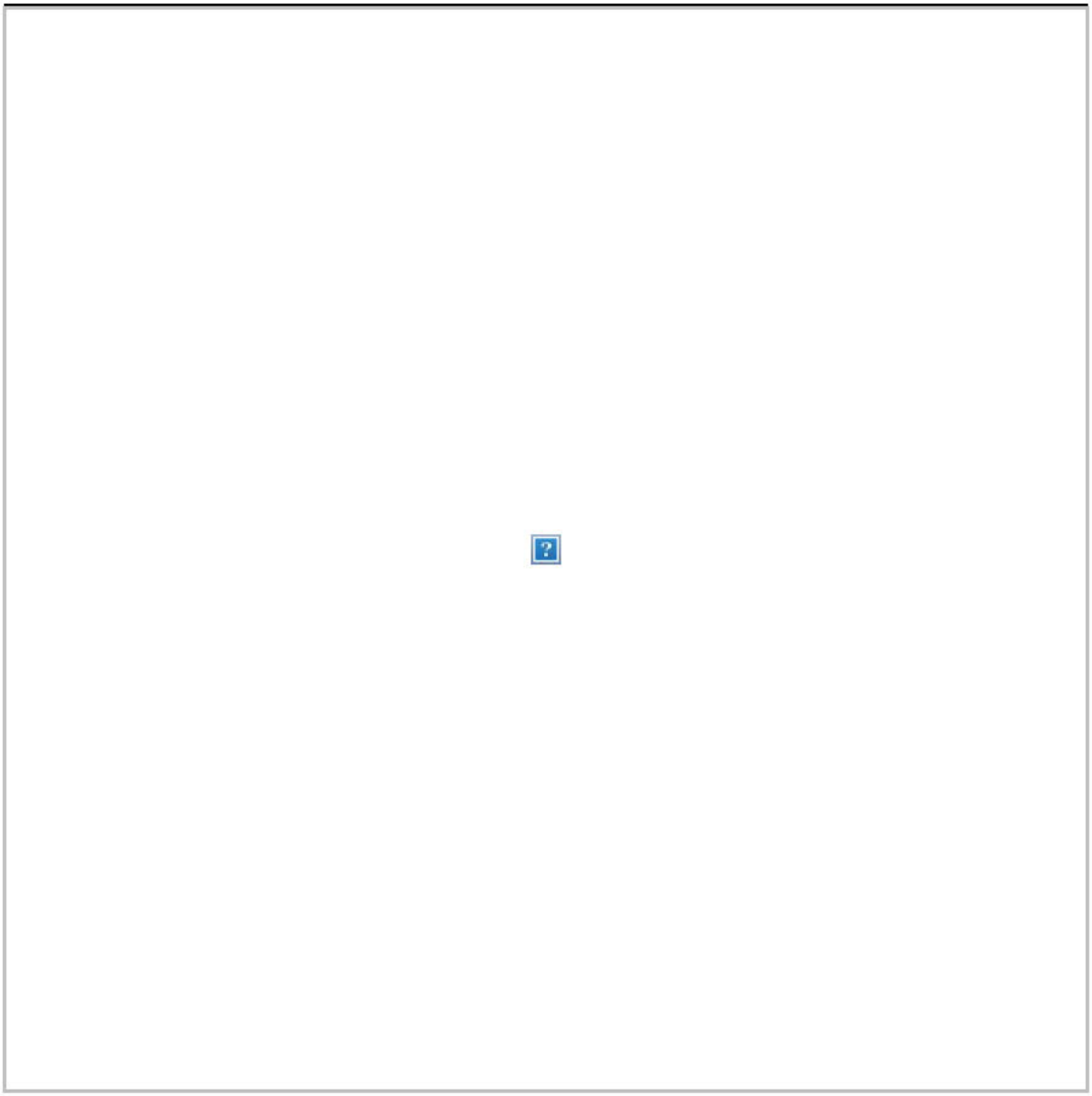
READ MORE

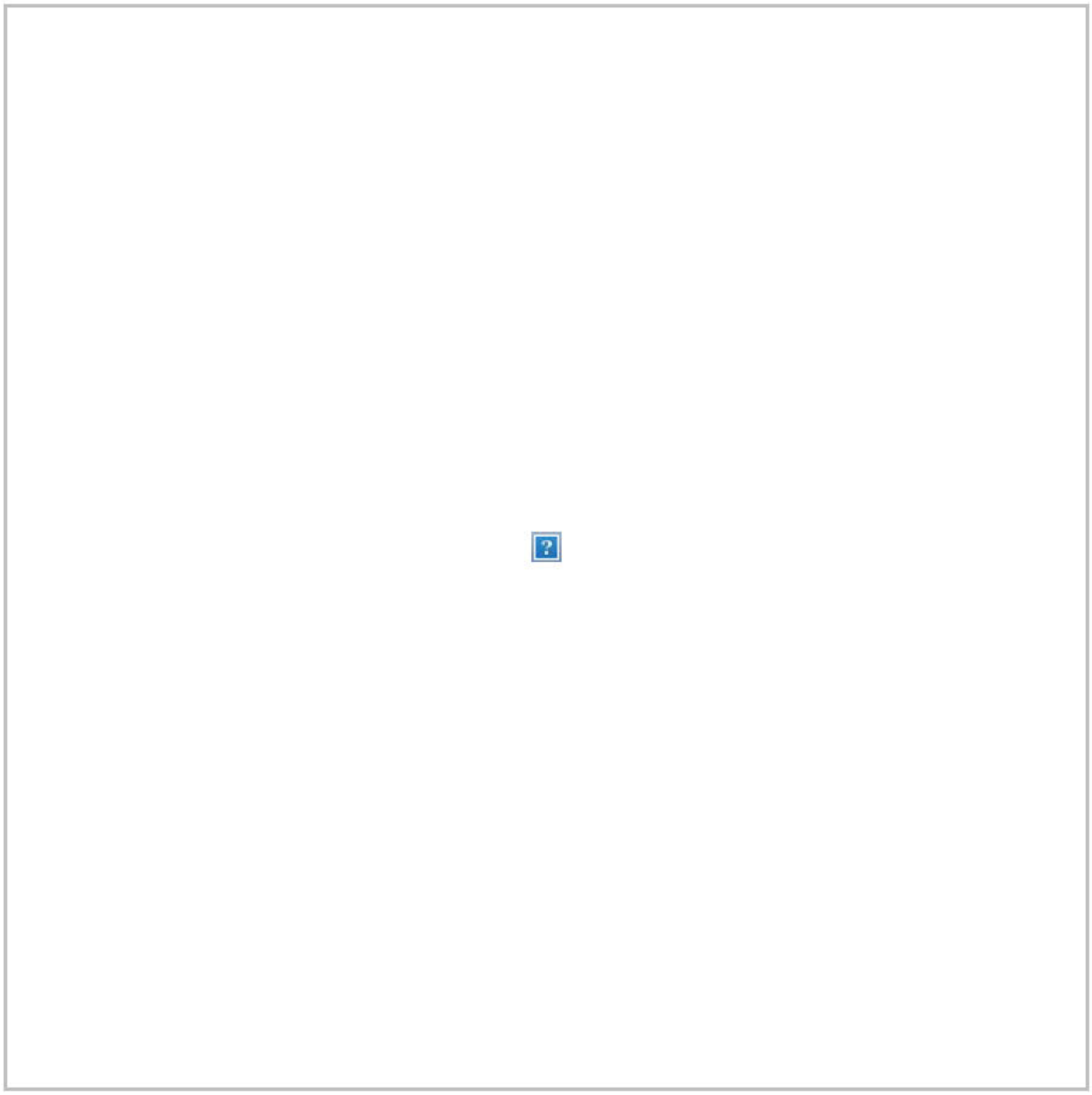


Multiphase ADS from SRL can cut queue lengths by 50%

A multiphase adaptive detection system (ADS) for portable and temporary traffic signals has been independently proven to reduce average queue lengths by 50%, potentially saving commuters more than one day a year of journey time.

READ MORE

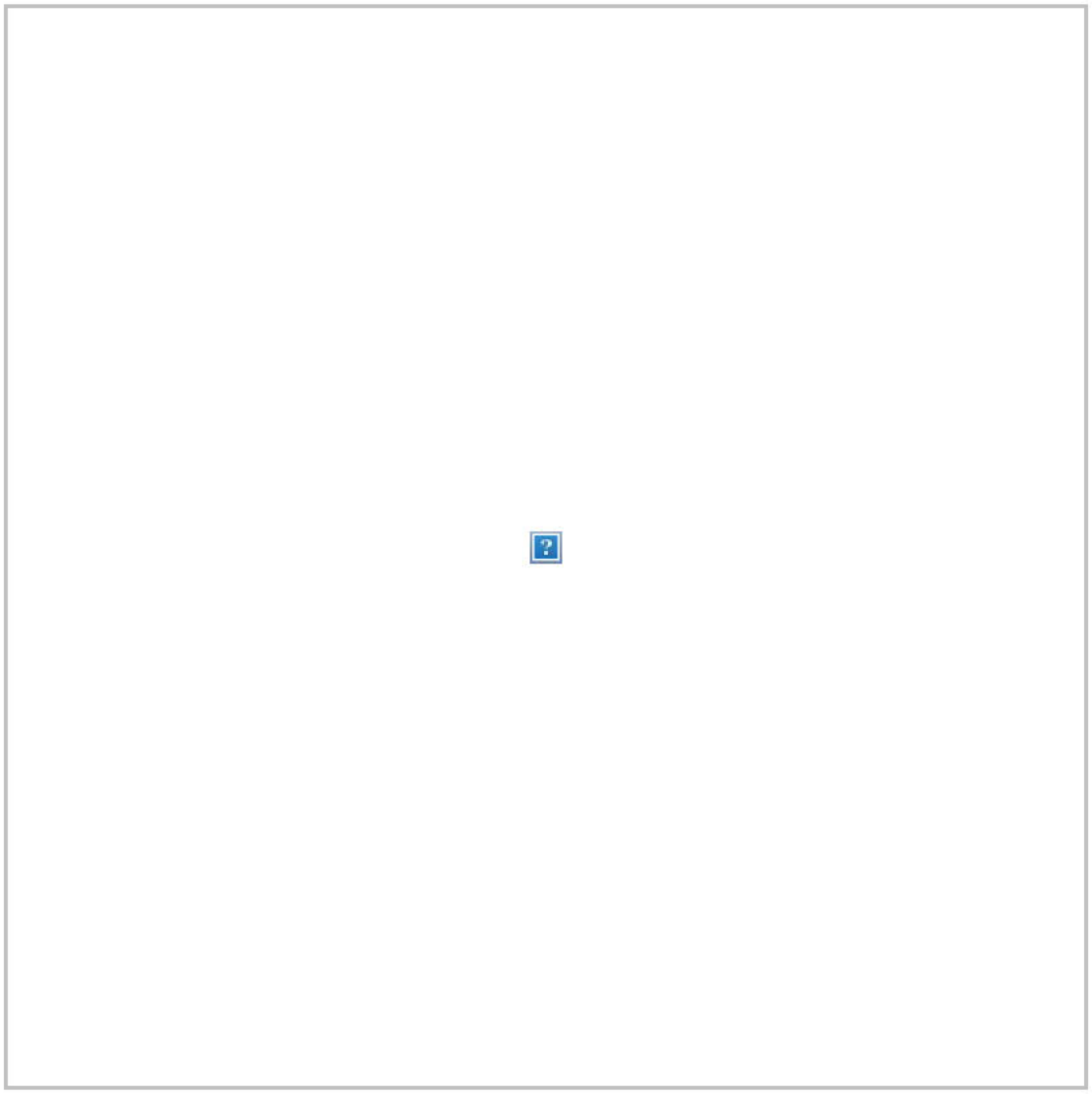




MORE NEWS…

- Data management platform from Commsignia optimizes V2X traffic management
- TIER partners with AI start-up Captur to encourage reporting of e-scooter misuse
- UK DfT allocates £15m to repair and upgrade traffic signals
- Waycare acquired by ALPR company Rekor Systems, for US$61M
- UK EV industry to benefit from innovative Monta app
- Iteris and Wejo partnership will increase safety and efficiency of CAVs
- New innovative technology will make London’s workzones safer and smarter





If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: ITS America prepares technical tour for first day of Annual Meeting
Date: Friday, December 3, 2021 8:36:12 AM

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

News from Traffic Technology International View this email online

Podcast Events Videos

ITS America prepares technical

tour for first day of Annual Meeting

Attendees to next week's (December 7-10) ITS America Annual Meeting in Charlotte, North Carolina, can look forward to an exclusive technical tour of the nearby I-77 Express Lanes Operations Center. Taking place on Tuesday, December 7 from 1pm – 3pm, the technical tour will be hosted by the North Carolina Department of Transportation (NCDOT), the North Carolina Turnpike Authority (NCTA), and I-77 Mobility Partners.



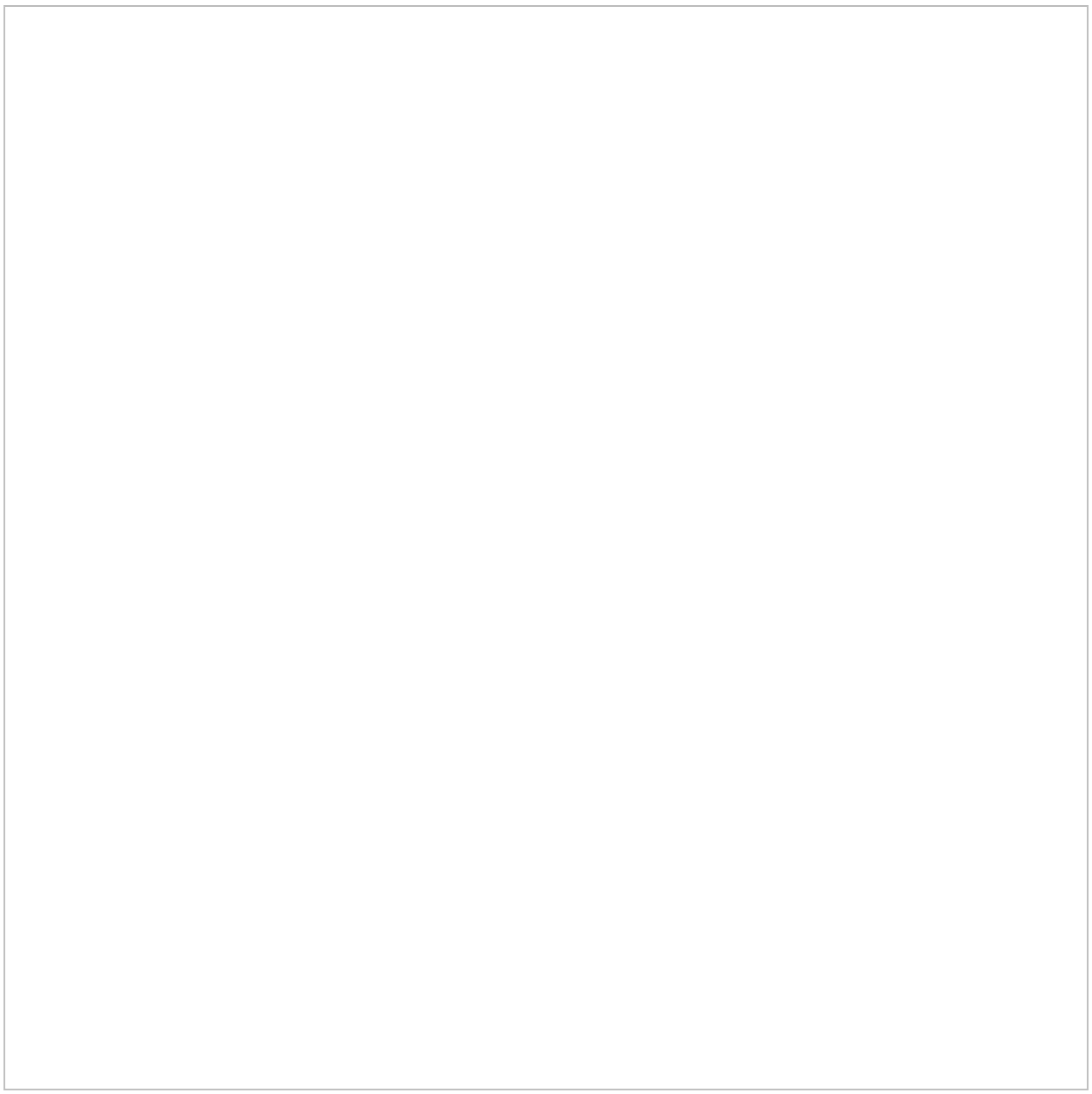
READ MORE

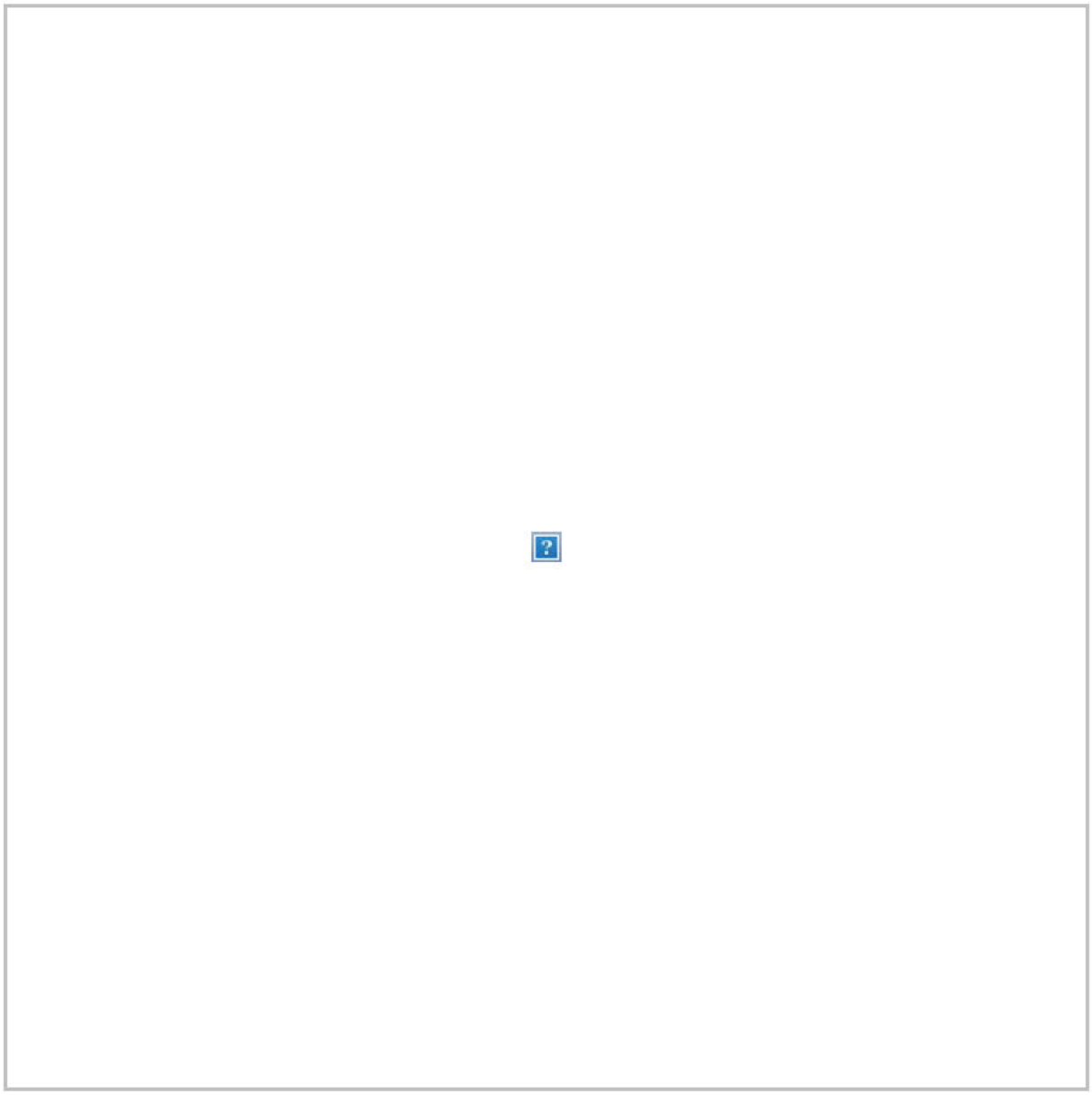


#ITSA2021: Industry-first traffic-cabinet lock to be showcased

At next week's ITS America Annual Meeting in Charlotte, North Carolina (December 7-10) 360ns will be showcasing its Smartlock 8000, bringing web control and card access to traffic cabinets, with no additional space required.

READ MORE







Podcast 19: The rise in road risk – an interview with David Braunstein

TTi editor Tom Stone talks to David Braunstein, president of Together for Safer Roads. David discusses the recent increase in road risk, near-miss analysis and minimising the distractions of smart phones. Plus news and conversation with Tom Stone and Saul Wordsworth.

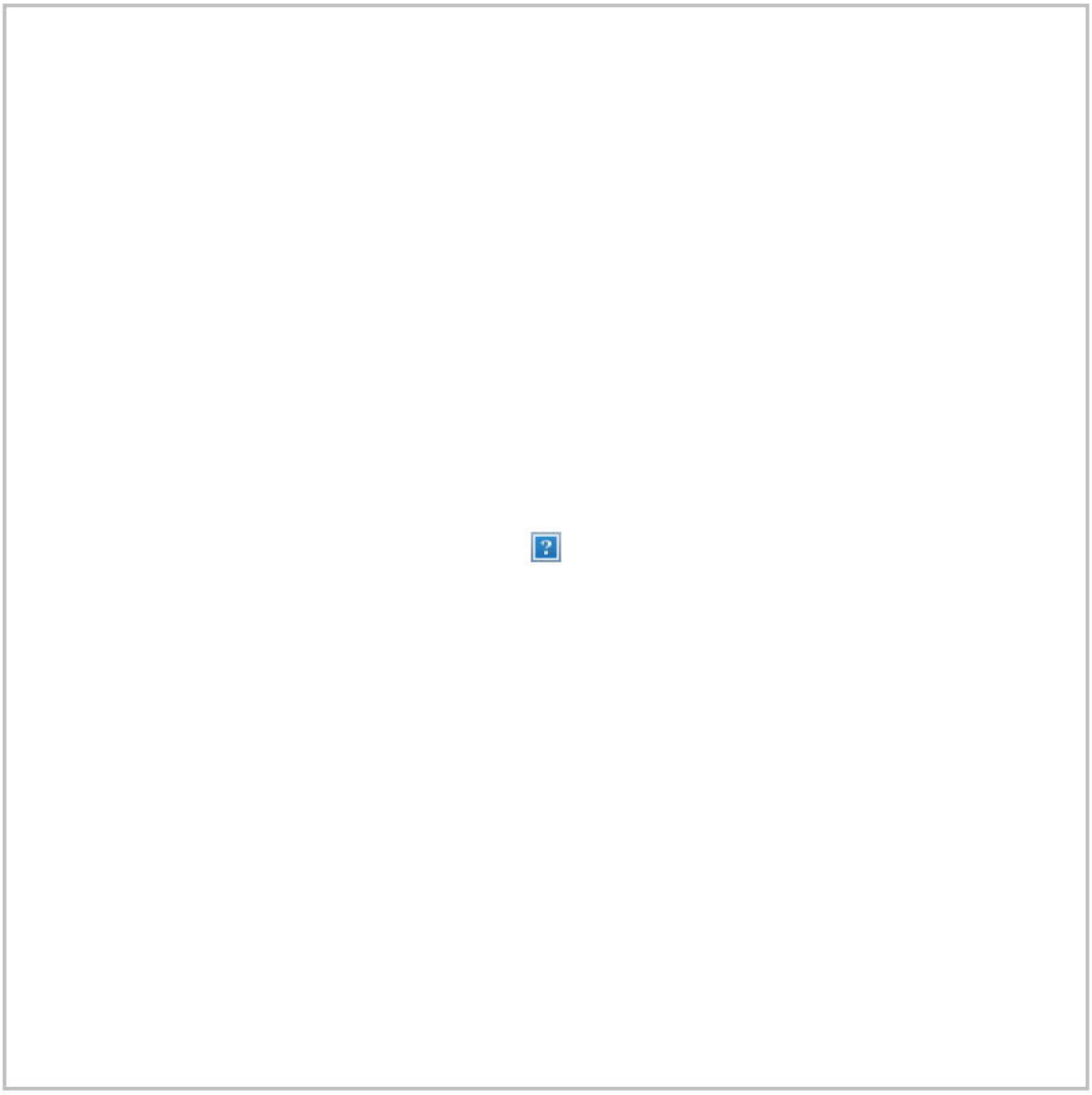
LISTEN

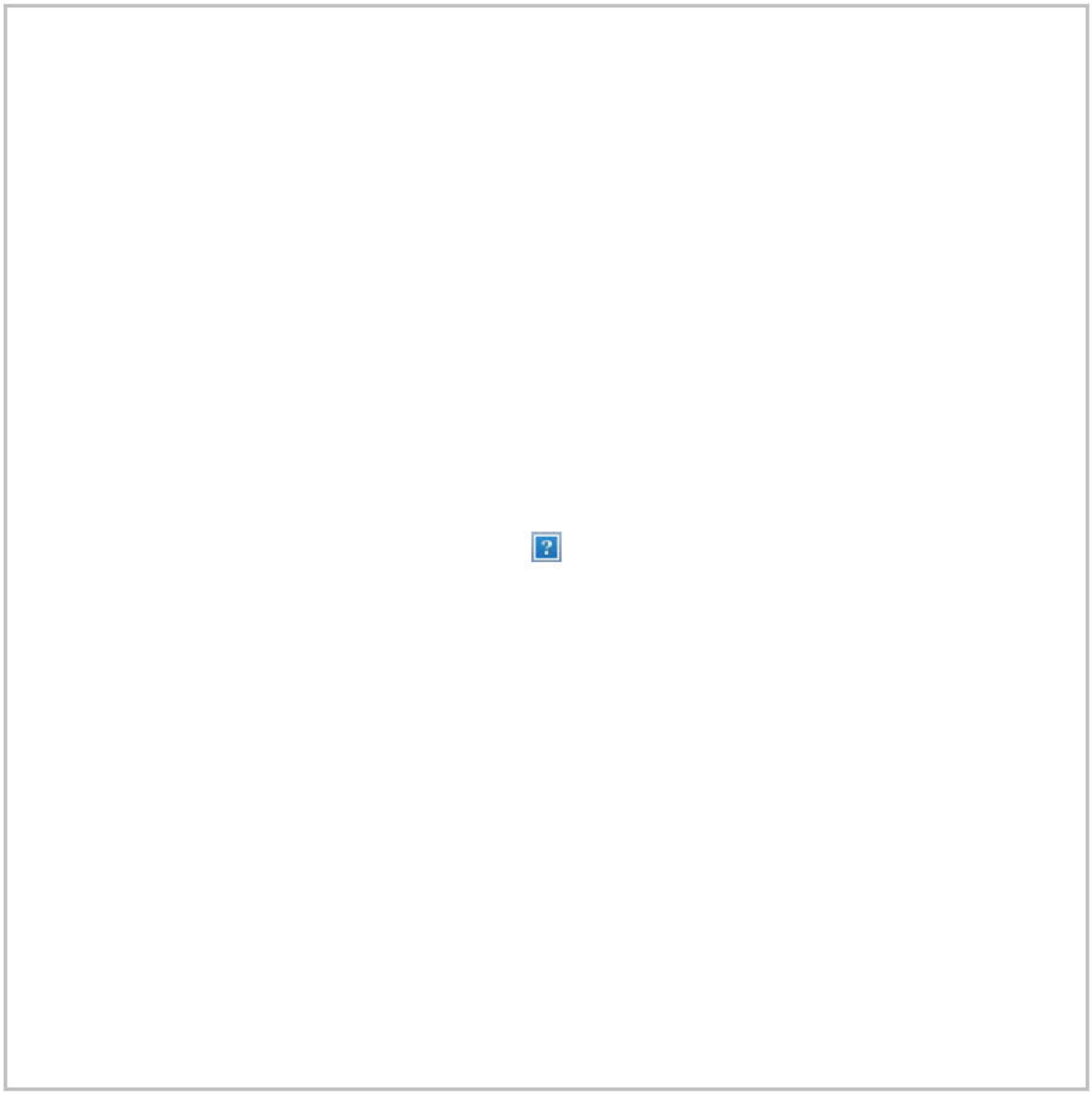


Carrida releases new version of Edge ALPR software

ALPR software solutions provider Carrida Technologies, has released version 4.7 of its Edge ALPR software, which includes numerous enhancements and new functionalities. These include support for three-digit alpha-3 country codes in accordance with ISO 3166-1.

READ MORE







Four new Jenoptik average speed camera schemes planned for UK

The first average speed schemes in Warwickshire are being introduced with a promise to not only improve safety and save lives but also improve traffic flows and air quality. The Jenoptik Specs cameras are to be installed along sections of the A435, A446, A426 and A428.

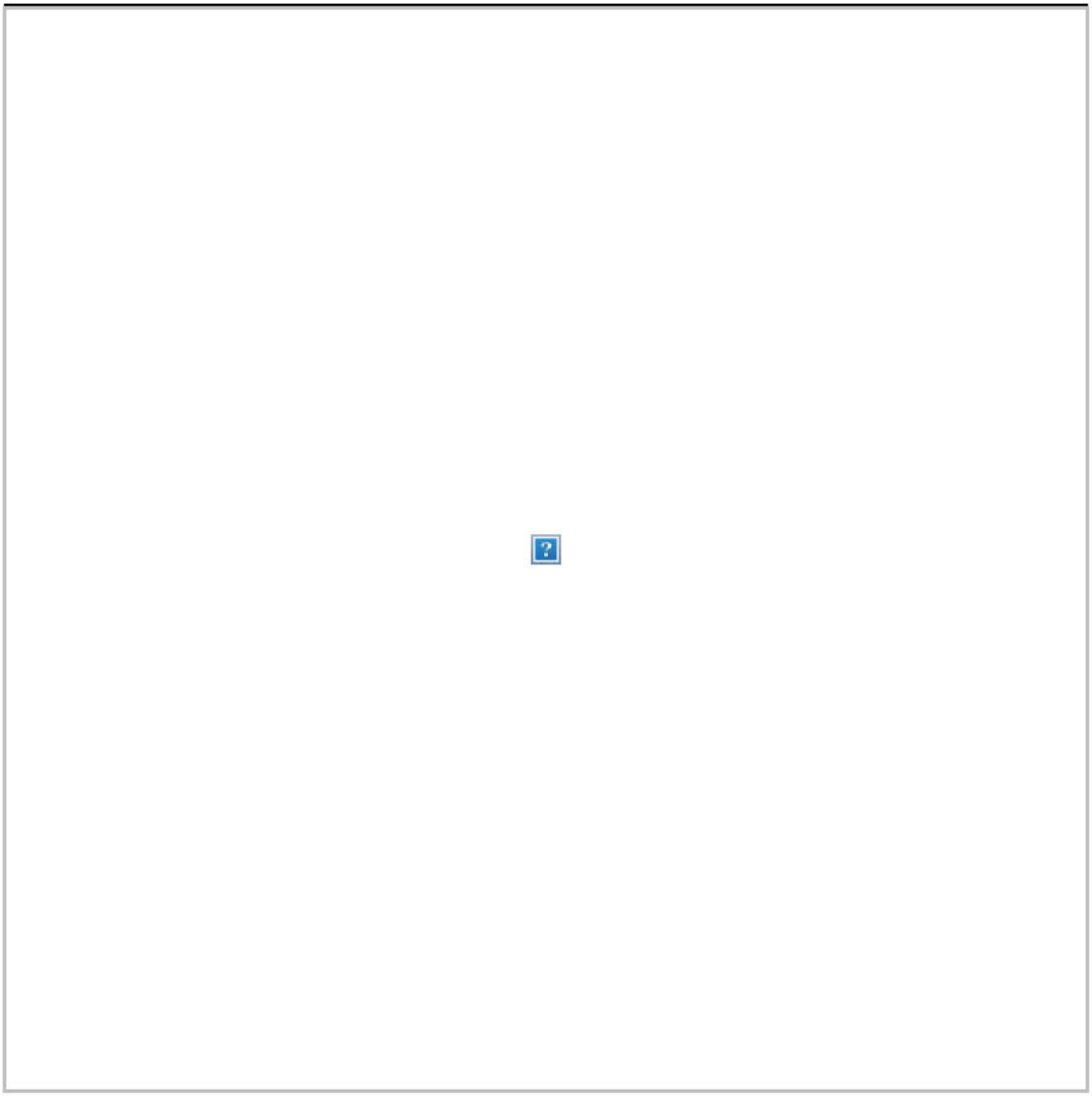
READ MORE

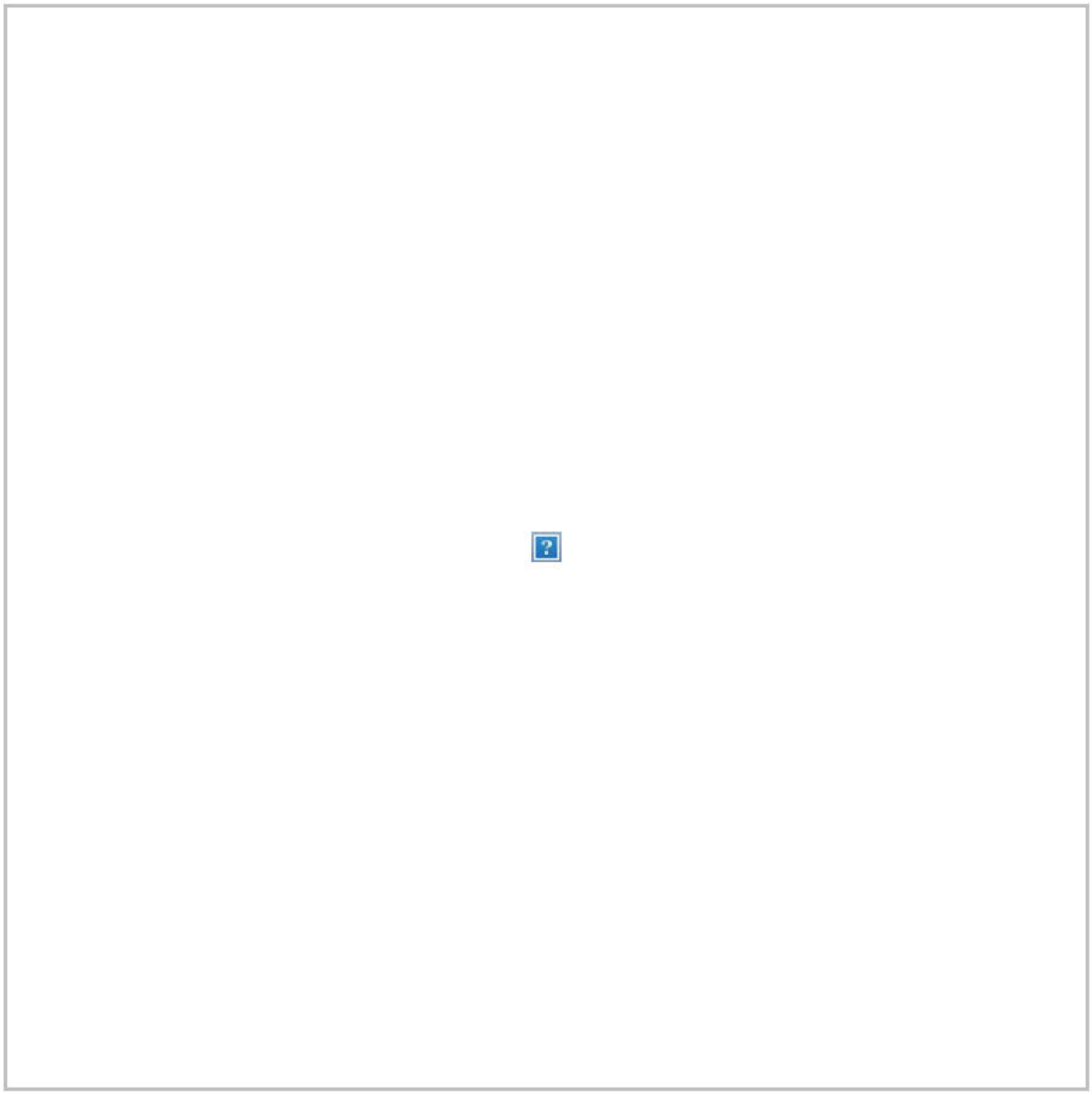


New, real-time smart parking system for Ghent, Belgium

The City of Ghent, Belgium, will implement a new dynamic traffic control system by mid-2022. The system will inform visitors in real time about the current parking situation, the occupancy rate of the various car parks, serious traffic disruptions and much more.

READ MORE







UK-first EV charging hub opened using Kempower technology

A UK-first electric vehicle (EV) dynamic charging hub has opened in Wolverhampton. The site is the first of over 150 charging hubs being delivered across the UK by Osprey Charging in a £75 million program to eliminate charging anxiety ahead of the 2030 ban on petrol and diesel cars.

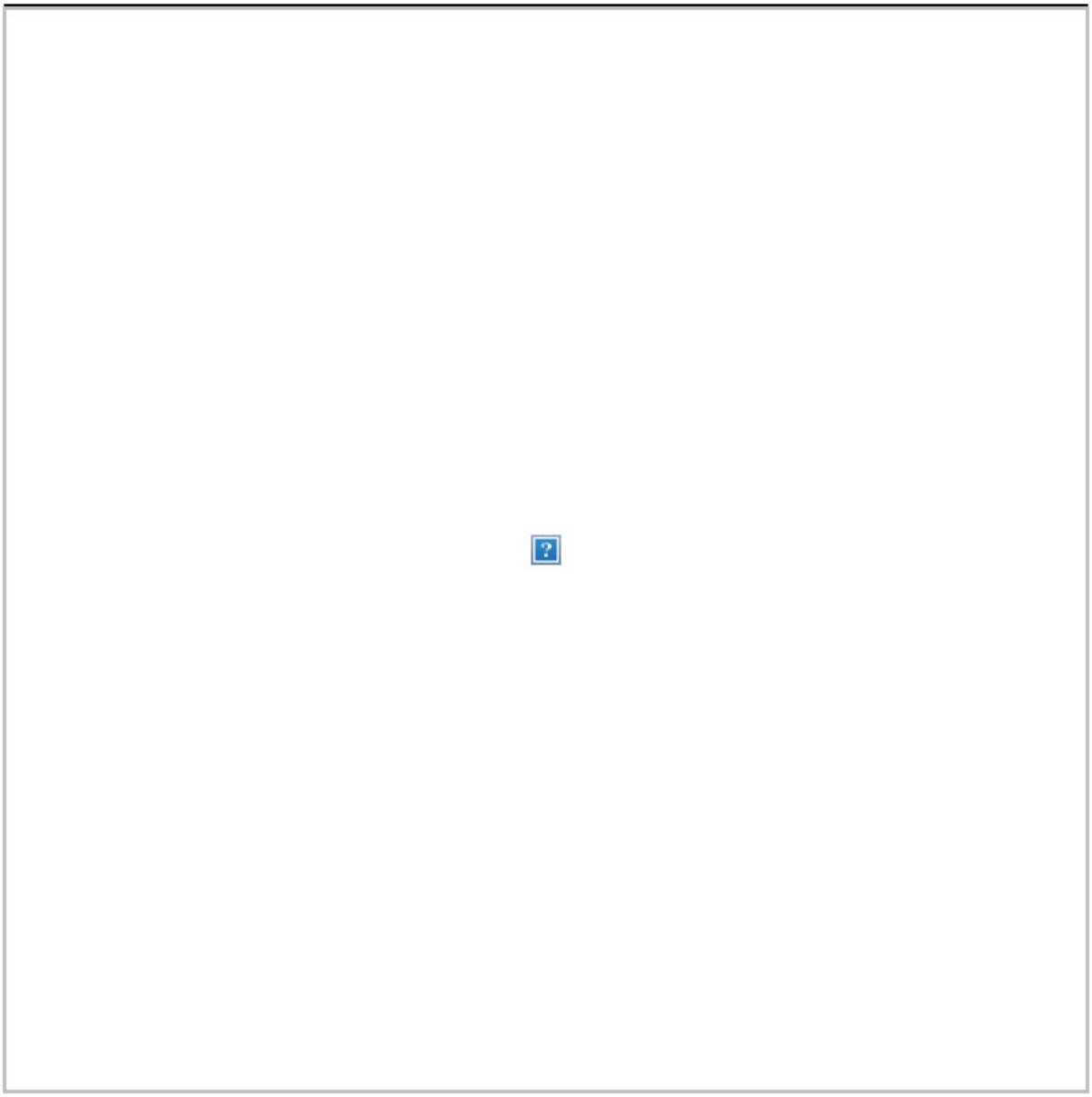
READ MORE



Iteris lands $1.4m task order to support smart mobility in Florida

Iteris has been awarded a $1.4 million task order from Metric Engineering to support the Florida Department of Transportation (FDOT) for a regional smart mobility, safety and sustainability program.

READ MORE



If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.



From: Axon
To: McCarthy, Steven (POL)
Subject: Join Axon and Flock for a can't-miss ALPR launch event
Date: Friday, August 27, 2021 2:09:45 PM

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

Axon logo

Product Launch Event

Axon will be joining Flock Safety's quarterly product launch on Wednesday, September 1, 2021 at 1 PM EST / 10 AM PST to discuss our disruptively affordable mobile and fixed ALPR partnership. Here's what you can expect at the event:

- Unveiling of an advanced evidence delivery package, including solutions for drug trafficking, motor vehicle theft and drive-by shooting investigations
- A live conversation with Axon's Director of Fleet Products, Blake Bullock, on fully-integrated fixed and mobile ALPR solutions for scalable, city-wide coverage with the new Fleet 3 in-car camera solution
- Inaugural #Solved Awards - nominate a fellow officer here, and we will announce the winners (and prizes) during the event

- Flock Safety's biggest announcement to date - don't miss it!

SAVE YOUR SPOT

See you there,

The Axon Team

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe

From: Lt. Frank Borelli, Editor
To: Ditata, Matthew (POL)
Subject: L.A. Man Flies Drone that Struck LAPD Helicopter
Date: Friday, January 15, 2021 2:05:14 PM

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

Newsday

January 15, 2021

TODAY'S NEWS

L.A. Man Flies Drone that Struck LAPD Helicopter

A Los Angeles man admitted in federal court Thursday that he flew a drone that struck a Los Angeles Police…

Jail Mail Fails K9's Sniff Test

An envelope mailed to a

'Do You Need Help?' Courageous Orlando Waitress Saves Child

Thomas County Jail inmate did not pass the sniff test.

from Extreme Abuse

As server Flavaine Carvalho waited on a family of four, she saw signs that something possibly wasn't quite right…

Woman Held Against Her Will Jumps from Moving Car Curing Police Chase

WASHINGTON-A woman who reportedly was being kept against her will jumped out of a moving car driven by a man…

NYPD Cop Stabbed in the Neck by Woman in Her Home

An NYPD cop was stabbed in the neck by an erratic Brooklyn woman inside her home.

SPONSORED CONTENT

FAR Officer Image4534x356

Webinar: Diagram Your Crime Scene in Record Time, Save Time, Energy

This webinar was originally held on December 16, 2020.It is now available for on-demand viewing.Register here!At…

Learn How Innovative Technology is Helping Law Enforcement Stay Connected

What if a user could carry a solution in a large backpack or by a handle like a briefcase/hardcase? How about a…

The Scheduling Solution – Speaking from Experience

Lt. Steve Lynk (Ret.) discusses how public safety administrators save time and money with officer and staff…

Faro

FARO Freestyle 2

Introducing the Freestyle 2 from FARO: One of the most advanced handheld 3D forensic scanners on the market,…

Outfit your 2020+ Ford Police Interceptor Utility with Gamber-Johnson's Full-Line of Solutions

Gamber-Johnson, a leader in mobile mounting equipment, offers bumper to bumper vehicle solutions for the 2020+…

FEATURED VIDEO

Emotional Procession in Washington for Fallen Capitol Police Officer Brian Sicknick

A hearse carrying the casket of Brian Sicknick, a U.S. Capitol Police Officer who died from injuries following the…

Bodycam Shows Cops Shooting Knife-Wielding Suspect at Chico Petco

** (Disclaimer: This video content is intended for educational and informational purposes only) ** Chico,…

Former NYPD Detective Examines Capitol Police Officer Eugene Goodman's Actions to Divert Rioters

Kirk Burkhalter, a former NYPD detective, examined the confrontation between Capitol police officer Eugene Goodman…

FEATURED PRODUCTS

Elkin



Ekin X Spotter

The Ekin X Spotter is a mobile speed enforcement, automatic license plate Recognition (ALPR) and traffic violation…

CN4P



Captain LX

A premier storage and organization solution, the Captain LX from TruckVault is a full-featured Command Center that…

Gamberjohnson



Samsung DEX Solutions

Today's mobile workers rely on having information available at a moment's notice whether they're on patrol, on…



Aker Leather 588 Swivel Radio Holders for Motorola

Aker Leather 588 Swivel Radio Holders are made in the USA using premium leather & feature a heavy-duty injection…

Browse duty gear @ akerleather.com

FEATURED CONTENT



20201230115143

Eye for Evidence

Evidence is an important role in every case. The intent of this blog is to provide helpful insight to strengthen…

Armorexpress

Equipment Resolutions for the New Year

Are there resolutions that law enforcement agencies could make that would be of ultimate benefit to all involved?

Navistar International Corp. Factory Attack

Fired six years earlier; convicted of theft from the company; divorced, and reporting for a federal prison term…

© 2021 All rights reserved, Endeavor Business Media, LLC.

This email is being sent to matthew.ditata@state.ma.us.

Please add news.officer.com and mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
331 54th Avenue N.
Nashville, TN 37209

From: Lt. Frank Borelli, Editor
To: zzLyver, Michael (POL)
Subject: L.A. Man Flies Drone that Struck LAPD Helicopter
Date: Friday, January 15, 2021 2:04:29 PM

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

Newsday

January 15, 2021

TODAY'S NEWS

L.A. Man Flies Drone that Struck LAPD Helicopter

A Los Angeles man admitted in federal court Thursday that he flew a drone that struck a Los Angeles Police…

Jail Mail Fails K9's Sniff Test

An envelope mailed to a

'Do You Need Help?' Courageous Orlando Waitress Saves Child

Thomas County Jail inmate did not pass the sniff test.

from Extreme Abuse

As server Flavaine Carvalho waited on a family of four, she saw signs that something possibly wasn't quite right…

Woman Held Against Her Will Jumps from Moving Car Curing Police Chase

WASHINGTON-A woman who reportedly was being kept against her will jumped out of a moving car driven by a man…

NYPD Cop Stabbed in the Neck by Woman in Her Home

An NYPD cop was stabbed in the neck by an erratic Brooklyn woman inside her home.

SPONSORED CONTENT

FAR Officer Image4534x356

Webinar: Diagram Your Crime Scene in Record Time, Save Time, Energy

This webinar was originally held on December 16, 2020.It is now available for on-demand viewing.Register here!At…

Learn How Innovative Technology is Helping Law Enforcement Stay Connected

What if a user could carry a solution in a large backpack or by a handle like a briefcase/hardcase? How about a…

The Scheduling Solution – Speaking from Experience

Lt. Steve Lynk (Ret.) discusses how public safety administrators save time and money with officer and staff…

Faro

FARO Freestyle 2

Introducing the Freestyle 2 from FARO: One of the most advanced handheld 3D forensic scanners on the market,…

Outfit your 2020+ Ford Police Interceptor Utility with Gamber-Johnson's Full-Line of Solutions

Gamber-Johnson, a leader in mobile mounting equipment, offers bumper to bumper vehicle solutions for the 2020+…

FEATURED VIDEO

Emotional Procession in Washington for Fallen Capitol Police Officer Brian Sicknick

A hearse carrying the casket of Brian Sicknick, a U.S. Capitol Police Officer who died from injuries following the…

Bodycam Shows Cops Shooting Knife-Wielding Suspect at Chico Petco

** (Disclaimer: This video content is intended for educational and informational purposes only) ** Chico,…

Former NYPD Detective Examines Capitol Police Officer Eugene Goodman's Actions to Divert Rioters

Kirk Burkhalter, a former NYPD detective, examined the confrontation between Capitol police officer Eugene Goodman…

FEATURED PRODUCTS

Elkin



Ekin X Spotter

The Ekin X Spotter is a mobile speed enforcement, automatic license plate Recognition (ALPR) and traffic violation…

CN4P



Captain LX

A premier storage and organization solution, the Captain LX from TruckVault is a full-featured Command Center that…

Gamberjohnson



Samsung DEX Solutions

Today's mobile workers rely on having information available at a moment's notice whether they're on patrol, on…



Aker Leather 588 Swivel Radio Holders for Motorola

Aker Leather 588 Swivel Radio Holders are made in the USA using premium leather & feature a heavy-duty injection…

Browse duty gear @ akerleather.com

FEATURED CONTENT



20201230115143

Eye for Evidence

Evidence is an important role in every case. The intent of this blog is to provide helpful insight to strengthen…

Armorexpress

Equipment Resolutions for the New Year

Are there resolutions that law enforcement agencies could make that would be of ultimate benefit to all involved?

Navistar International Corp. Factory Attack

Fired six years earlier; convicted of theft from the company; divorced, and reporting for a federal prison term…

© 2021 All rights reserved, Endeavor Business Media, LLC.

This email is being sent to michael.lyver@pol.state.ma.us.

Please add news.officer.com and mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
331 54th Avenue N.
Nashville, TN 37209

From: Lt. Frank Borelli, Editor
To: Walsh, Stephen C (POL)
Subject: L.A. Man Flies Drone that Struck LAPD Helicopter
Date: Friday, January 15, 2021 2:03:30 PM

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

Newsday

January 15, 2021

TODAY'S NEWS

L.A. Man Flies Drone that Struck LAPD Helicopter

A Los Angeles man admitted in federal court Thursday that he flew a drone that struck a Los Angeles Police…

Jail Mail Fails K9's Sniff Test

An envelope mailed to a

'Do You Need Help?' Courageous Orlando Waitress Saves Child

Thomas County Jail inmate did not pass the sniff test.

from Extreme Abuse

As server Flavaine Carvalho waited on a family of four, she saw signs that something possibly wasn't quite right…

Woman Held Against Her Will Jumps from Moving Car Curing Police Chase

WASHINGTON-A woman who reportedly was being kept against her will jumped out of a moving car driven by a man…

NYPD Cop Stabbed in the Neck by Woman in Her Home

An NYPD cop was stabbed in the neck by an erratic Brooklyn woman inside her home.

SPONSORED CONTENT

FAR Officer Image4534x356

Webinar: Diagram Your Crime Scene in Record Time, Save Time, Energy

This webinar was originally held on December 16, 2020.It is now available for on-demand viewing.Register here!At…

Learn How Innovative Technology is Helping Law Enforcement Stay Connected

What if a user could carry a solution in a large backpack or by a handle like a briefcase/hardcase? How about a…

The Scheduling Solution – Speaking from Experience

Lt. Steve Lynk (Ret.) discusses how public safety administrators save time and money with officer and staff…

Faro

FARO Freestyle 2

Introducing the Freestyle 2 from FARO: One of the most advanced handheld 3D forensic scanners on the market,…

Outfit your 2020+ Ford Police Interceptor Utility with Gamber-Johnson's Full-Line of Solutions

Gamber-Johnson, a leader in mobile mounting equipment, offers bumper to bumper vehicle solutions for the 2020+…

FEATURED VIDEO

Emotional Procession in Washington for Fallen Capitol Police Officer Brian Sicknick

A hearse carrying the casket of Brian Sicknick, a U.S. Capitol Police Officer who died from injuries following the…

Bodycam Shows Cops Shooting Knife-Wielding Suspect at Chico Petco

** (Disclaimer: This video content is intended for educational and informational purposes only) ** Chico,…

Former NYPD Detective Examines Capitol Police Officer Eugene Goodman's Actions to Divert Rioters

Kirk Burkhalter, a former NYPD detective, examined the confrontation between Capitol police officer Eugene Goodman…

FEATURED PRODUCTS

Elkin

Ekin X Spotter

The Ekin X Spotter is a mobile speed enforcement, automatic license plate Recognition (ALPR) and traffic violation…

CN4P

Captain LX

A premier storage and organization solution, the Captain LX from TruckVault is a full-featured Command Center that…

Gamberjohnson

Samsung DEX Solutions

Today's mobile workers rely on having information available at a moment's notice whether they're on patrol, on…

Aker Leather 588 Swivel Radio Holders for Motorola

Aker Leather 588 Swivel Radio Holders are made in the USA using premium leather & feature a heavy-duty injection…

Browse duty gear @ akerleather.com

FEATURED CONTENT

20201230115143

Eye for Evidence

Evidence is an important role in every case. The intent of this blog is to provide helpful insight to strengthen…

Armorexpress

Equipment Resolutions for the New Year

Are there resolutions that law enforcement agencies could make that would be of ultimate benefit to all involved?

Navistar International Corp. Factory Attack

Fired six years earlier; convicted of theft from the company; divorced, and reporting for a federal prison term…

© 2021 All rights reserved, Endeavor Business Media, LLC.

This email is being sent to stephen.walsh@pol.state.ma.us.

Please add news.officer.com and mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
331 54th Avenue N.
Nashville, TN 37209

From: Lt. Frank Borelli, Editor
To: Baptiste, Walter (POL)
Subject: L.A. Man Flies Drone that Struck LAPD Helicopter
Date: Friday, January 15, 2021 2:09:29 PM

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

Newsday

January 15, 2021

TODAY'S NEWS

L.A. Man Flies Drone that Struck LAPD Helicopter

A Los Angeles man admitted in federal court Thursday that he flew a drone that struck a Los Angeles Police…

Jail Mail Fails K9's Sniff Test

An envelope mailed to a

'Do You Need Help?' Courageous Orlando Waitress Saves Child

Thomas County Jail inmate did not pass the sniff test.

from Extreme Abuse

As server Flavaine Carvalho waited on a family of four, she saw signs that something possibly wasn't quite right…

Woman Held Against Her Will Jumps from Moving Car Curing Police Chase

WASHINGTON-A woman who reportedly was being kept against her will jumped out of a moving car driven by a man…

NYPD Cop Stabbed in the Neck by Woman in Her Home

An NYPD cop was stabbed in the neck by an erratic Brooklyn woman inside her home.

SPONSORED CONTENT

FAR Officer Image4534x356

Webinar: Diagram Your Crime Scene in Record Time, Save Time, Energy

This webinar was originally held on December 16, 2020.It is now available for on-demand viewing.Register here!At…

Learn How Innovative Technology is Helping Law Enforcement Stay Connected

What if a user could carry a solution in a large backpack or by a handle like a briefcase/hardcase? How about a…

The Scheduling Solution – Speaking from Experience

Lt. Steve Lynk (Ret.) discusses how public safety administrators save time and money with officer and staff…

Faro

FARO Freestyle 2

Introducing the Freestyle 2 from FARO: One of the most advanced handheld 3D forensic scanners on the market,…

Outfit your 2020+ Ford Police Interceptor Utility with Gamber-Johnson's Full-Line of Solutions

Gamber-Johnson, a leader in mobile mounting equipment, offers bumper to bumper vehicle solutions for the 2020+…

FEATURED VIDEO

Emotional Procession in Washington for Fallen Capitol Police Officer Brian Sicknick

A hearse carrying the casket of Brian Sicknick, a U.S. Capitol Police Officer who died from injuries following the…

Bodycam Shows Cops Shooting Knife-Wielding Suspect at Chico Petco

** (Disclaimer: This video content is intended for educational and informational purposes only) ** Chico,…

Former NYPD Detective Examines Capitol Police Officer Eugene Goodman's Actions to Divert Rioters

Kirk Burkhalter, a former NYPD detective, examined the confrontation between Capitol police officer Eugene Goodman…

FEATURED PRODUCTS

Elkin



Ekin X Spotter

The Ekin X Spotter is a mobile speed enforcement, automatic license plate Recognition (ALPR) and traffic violation…

CN4P



Captain LX

A premier storage and organization solution, the Captain LX from TruckVault is a full-featured Command Center that…

Gamberjohnson



Samsung DEX Solutions

Today's mobile workers rely on having information available at a moment's notice whether they're on patrol, on…



Aker Leather 588 Swivel Radio Holders for Motorola

Aker Leather 588 Swivel Radio Holders are made in the USA using premium leather & feature a heavy-duty injection…

Browse duty gear @ akerleather.com

FEATURED CONTENT



20201230115143

Eye for Evidence

Evidence is an important role in every case. The intent of this blog is to provide helpful insight to strengthen…

Armorexpress

Equipment Resolutions for the New Year

Are there resolutions that law enforcement agencies could make that would be of ultimate benefit to all involved?

Navistar International Corp. Factory Attack

Fired six years earlier; convicted of theft from the company; divorced, and reporting for a federal prison term…

© 2021 All rights reserved, Endeavor Business Media, LLC.

This email is being sent to walter.baptiste@pol.state.ma.us.

Please add news.officer.com and mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer
Endeavor Business Media
331 54th Avenue N.
Nashville, TN 37209

From: The Axon Team
To: McCarthy, Steven (POL)
Subject: Last chance to be part of a Fleet 3 milestone with us! Register now
Date: Tuesday, June 29, 2021 1:09:48 PM

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

Axon

Fleet 3 is coming, and it's changing the game. With integrated ALPR, more real-time data and situational awareness than ever before, and best-in-class hardware, our next in-car camera system is hitting the road. We want to tell you about it - but we also want to hear from you about it.

Join Rick Smith, Chief Executive Officer, Jeff Kunins, Chief Product Officer, and Blake Bullock, Director of Fleet Products, for an Ask Me Anything-style webinar about Fleet 3.

We can't wait to hear what you want to know!

REGISTER NOW

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe



From: The Axon Team
To: McCarthy, Steven (POL)
Subject: Last chance to be part of a Fleet 3 milestone with us! Register now
Date: Tuesday, June 29, 2021 1:10:00 PM

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

Axon

Fleet 3 is coming, and it's changing the game. With integrated ALPR, more real-time data and situational awareness than ever before, and best-in-class hardware, our next in-car camera system is hitting the road. We want to tell you about it - but we also want to hear from you about it.

Join Rick Smith, Chief Executive Officer, Jeff Kunins, Chief Product Officer, and Blake Bullock, Director of Fleet Products, for an Ask Me Anything-style webinar about Fleet 3.

We can't wait to hear what you want to know!

REGISTER NOW

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe



From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: LAST CHANCE: Addressing Ethics and Privacy in Police Technology Webinar
Date: Monday, August 9, 2021 9:13:55 AM

AxonWebinar8.10.2021.jpg

LAST CHANCE TO REGISTER!

Technology is evolving at a faster rate than ever. Simultaneously, public concern over government surveillance and intrusions on privacy rights are also growing. Axon (Formerly TASER International) has successfully introduced some of the most impactful – and controversial public safety technologies of the past 25 years including TASER weapons, body cameras, cloud software, and artificial intelligence based software services including automated license plate recognition (ALPR).

Join Rick Smith, CEO, Director, and Founder Axon (Formerly TASER

International) and Regina Holloway, Vice President of Community Impact at Axon, who will share insights and lessons learned in navigating issues related to public perceptions, ethics and privacy protections, and community engagement as critical elements in introducing new public safety technologies.

Register Now!

Presenters

Rick_Smith.jpeg

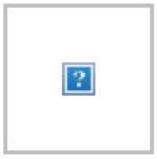
Rick Smith
Founder & CEO, Axon Enterprise

Rick Smith has served as Chief Executive Officer and as a director of the Company since 1993. He is a co-founder of the Company. After graduating from Harvard Cum Laude in just three years (class of 1991), Mr. Smith entered directly into the Masters of Business Administration Program at the University of Chicago, the youngest person accepted into his class at the business school. In two years, he completed both his M.B.A. with honors at the University of Chicago (normally a two-year program in itself) graduating in the top 5% of his class and a Masters Degree in International Finance from the University of Leuven in Leuven, Belgium. After graduating from graduate school in the summer of 1993, he immediately co-founded TASER International with his brother on September 7th of 1993. The company changed its name to Axon in April 2017 when the revenue bookings for their cloud software and wearable sensors business unit surpassed the scale of the original TASER weapons segment.

Regina Holloway
VP Community Relations, Axon Enterprise

Regina Holloway is the VP of Community Impact at Axon. Previously Regina was a Sr. Program Manager at the Policing Project at NYU School of Law, where she helped to implement the Neighborhood Policing Initiative in the City of Chicago. Before joining the Policing Project, Regina served as a Supervising

Investigator with the Civilian Office of Police Accountability in Chicago. There, she supervised a Major Case Squad which investigated officer-involved shootings. She began her legal career as a Clinical Fellow at Suffolk University Law School, where she developed housing discrimination investigations. That work led to the publication of a study on housing discrimination experienced by trans and gender non-conforming residents in the Boston area. The study was published in Yale Law School's Journal of Law and Feminism. Thereafter, Regina practiced criminal defense in the Boston District Courts, where she worked as a Bar Advocate for Suffolk Lawyers for Justice. Regina is a Senior Atlantic Fellow for Racial Equity through a partnership between Columbia University and the Nelson Mandela Foundation. She holds a Bachelor of Arts in Political Science and African-American Studies from Temple University and earned her Doctor of Jurisprudence from Suffolk University Law School.





LEARN MORE

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

UNSUBSCRIBING from this email will STOP ALL EMAILS from the FBINAA

You can edit your Communication Preferences from your Profile on the FBINAA Website.

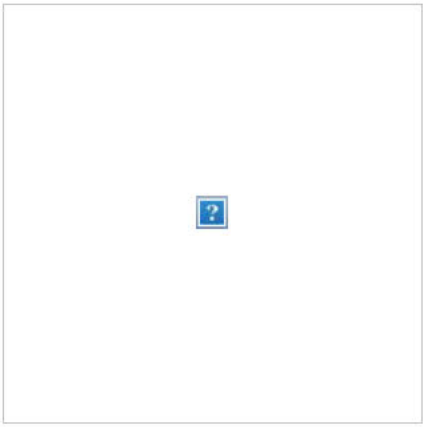
Share This Email | Share This Email | Share This Email | Share This Email

FBI National Academy Associates, Inc. | FBI Academy, Building 8-102, Quantico, VA 22135

Unsubscribe steven.mccarthy@pol.state.ma.us

About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with

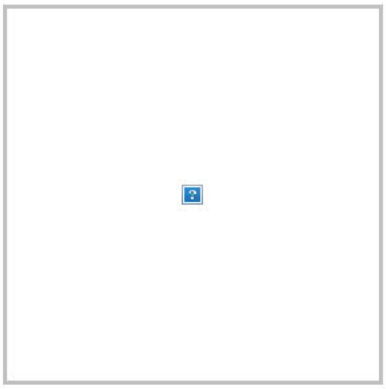


Try email marketing for free today!

From: Police1 Roll Call
To: Upton, Paul (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:06:02 PM

August 16, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

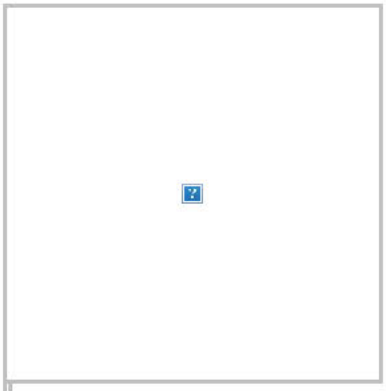
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience



What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation

Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



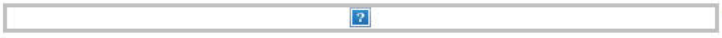
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

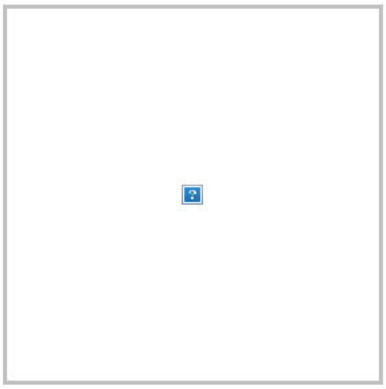
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzLee, Brian (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:05:45 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

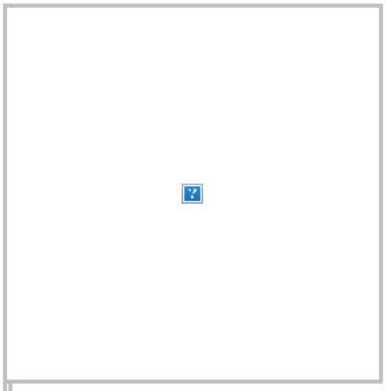
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

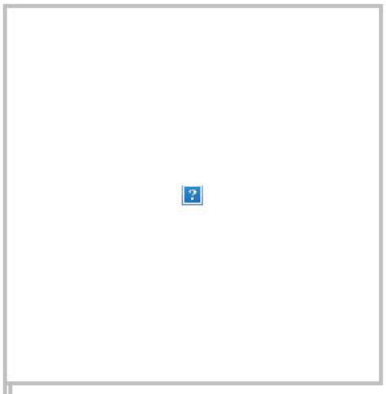


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

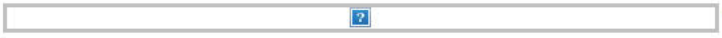


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

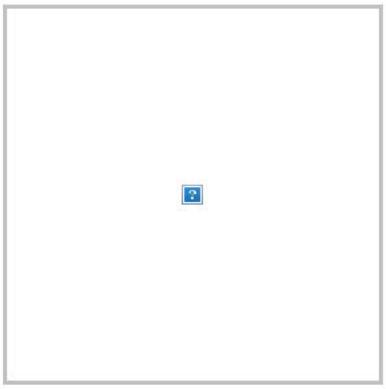
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: benesh_meghann E (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:05:29 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

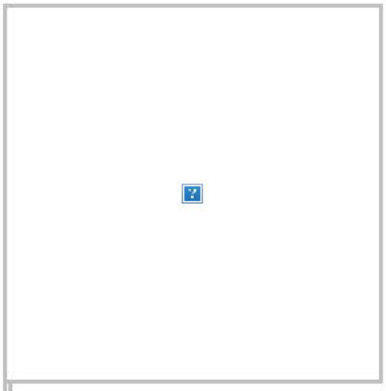
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

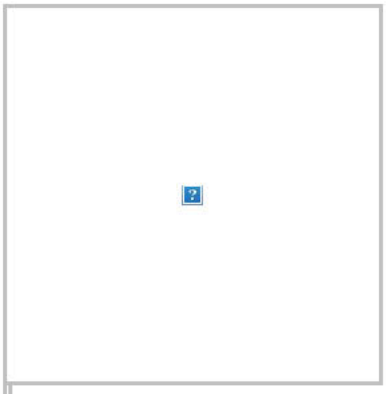


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



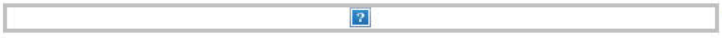
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

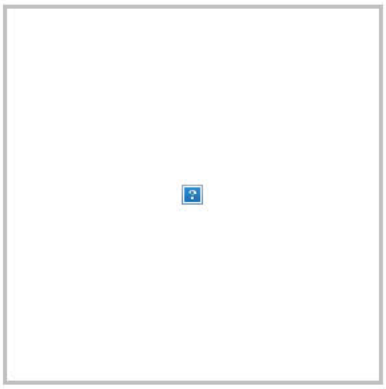
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cronin, John E (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:05:04 PM

August 16, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

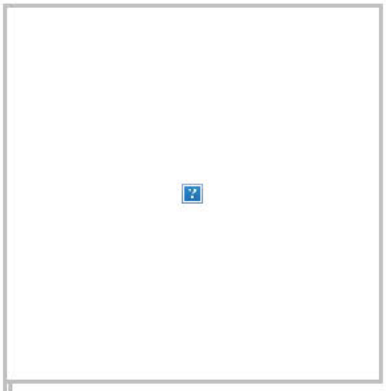
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

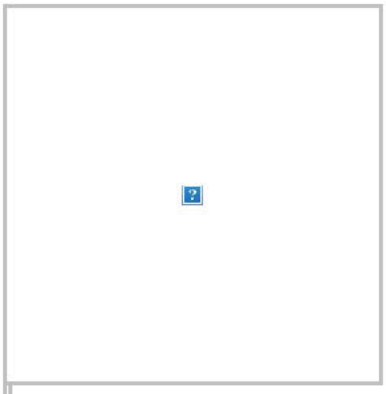


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



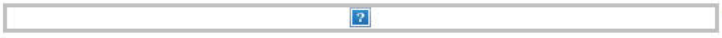
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

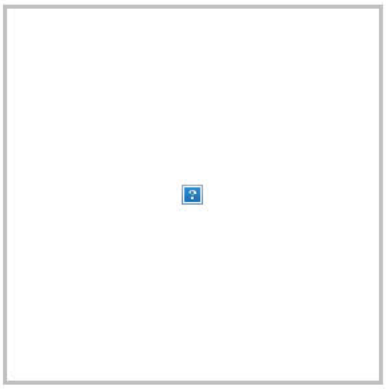
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Grassia, Michael (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:04:44 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

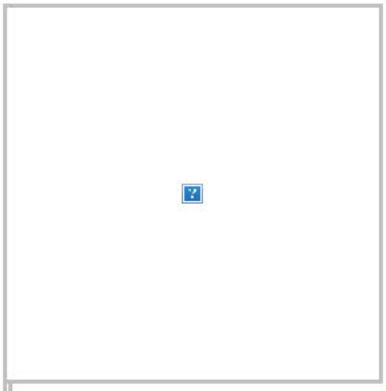
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

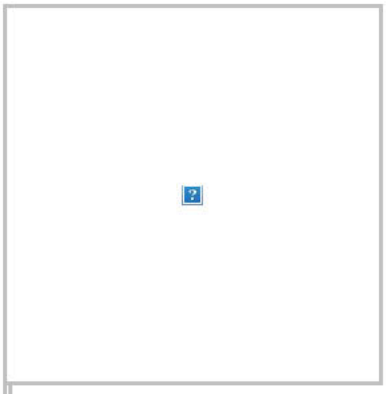


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



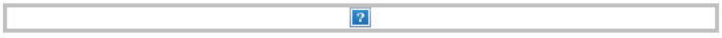
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB

MPD Entry-Level & Reserve Officer Positions Available - Apply Today!
Apply now

FEATURED VIDEO

7 things to look for in an in-car video system
Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

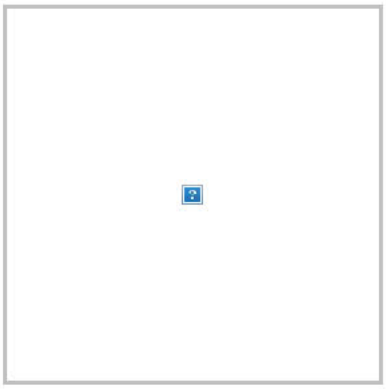
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzJohnson_Robert - Captain (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:03:38 PM

August 16, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

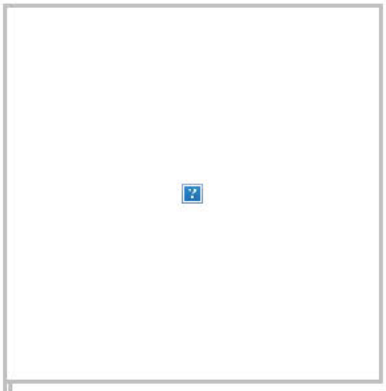
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

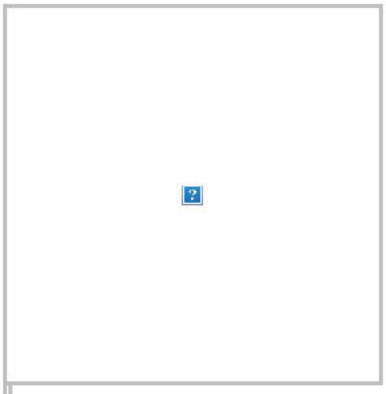


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



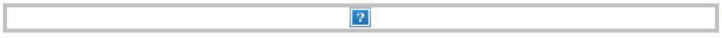
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

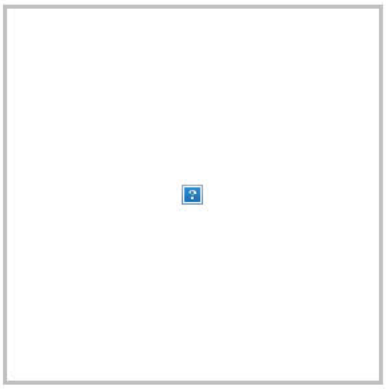
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Golenski, Michael (POL)
Subject: LEO LODDs in N.C., Mich.; Sacramento's "vaccinate or terminate" policy
Date: Monday, August 16, 2021 2:11:19 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

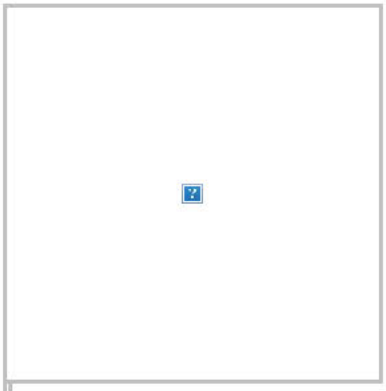
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

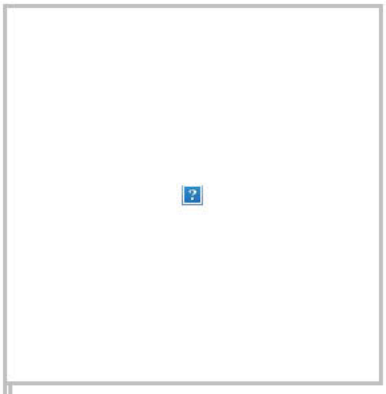


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

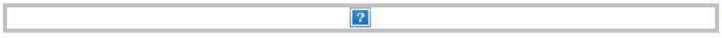


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

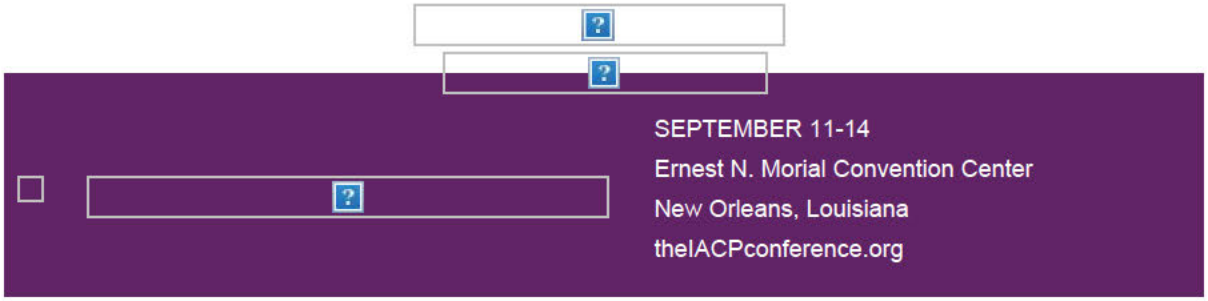
If you do not want to receive this newsletter, you can **opt-out here.**

If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Alert
To: Zimmerman, Amanda (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:52:15 AM

Having trouble viewing this email? View it in your browser.



Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Leger, Jessica (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:52:13 AM

Having trouble viewing this email? View it in your browser.

SEPTEMBER 11-14
Ernest N. Morial Convention Center
New Orleans, Louisiana
theIACPconference.org

Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

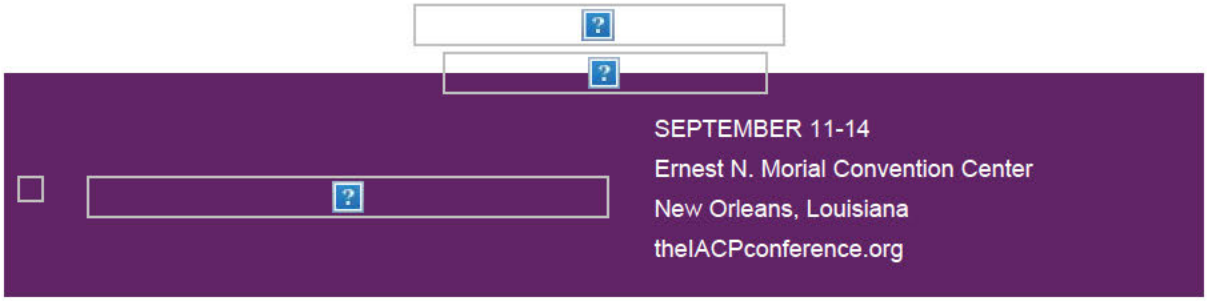
---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Mcginn, Daniel (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:35:09 AM

Having trouble viewing this email? View it in your browser.



Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Pirrotta, Melissa S. (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:06:57 AM

Having trouble viewing this email? View it in your browser.

SEPTEMBER 11-14
Ernest N. Morial Convention Center
New Orleans, Louisiana
theIACPconference.org

Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

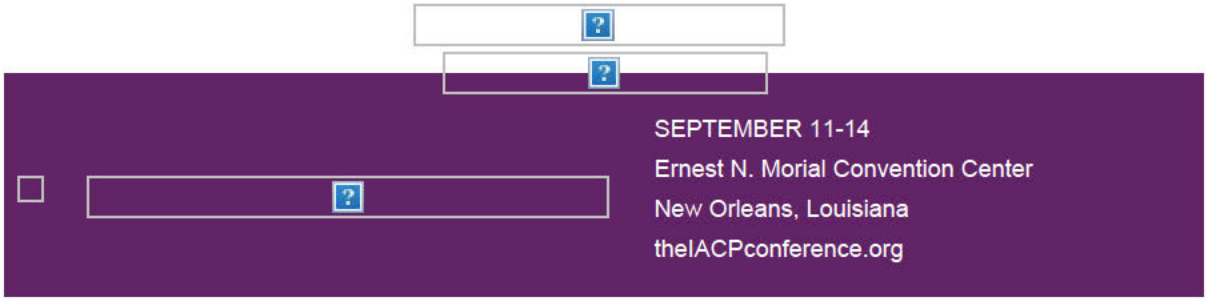
---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Tucker, Sheila (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:06:54 AM

Having trouble viewing this email? View it in your browser.



Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Thomas, Randy (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:06:41 AM

Having trouble viewing this email? View it in your browser.

SEPTEMBER 11-14
Ernest N. Morial Convention Center
New Orleans, Louisiana
theIACPconference.org

Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

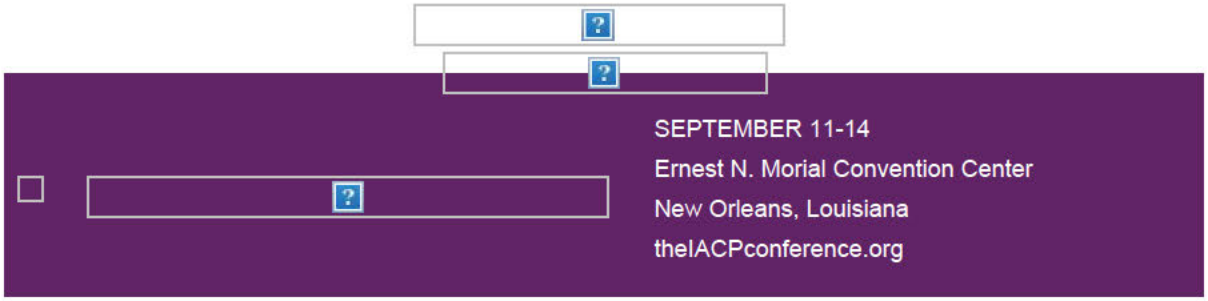
---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Tirella, Orlando (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:05:44 AM

Having trouble viewing this email? View it in your browser.



Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Wilcox, Christopher (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:04:20 AM

Having trouble viewing this email? View it in your browser.

SEPTEMBER 11-14
Ernest N. Morial Convention Center
New Orleans, Louisiana
theIACPconference.org

Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

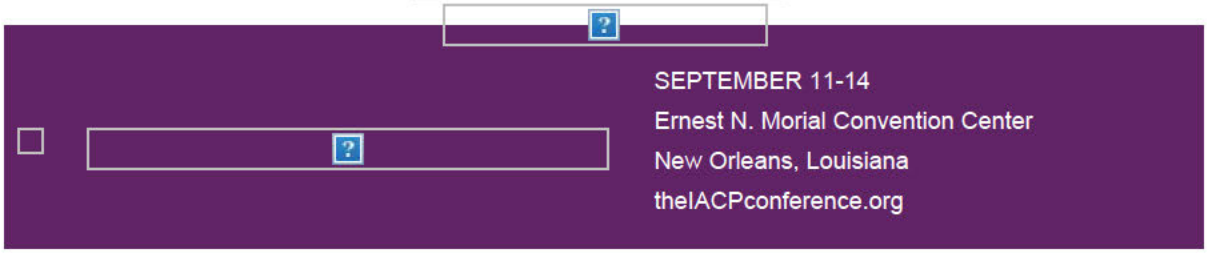
---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Mcginn, Daniel (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:04:10 AM

Having trouble viewing this email? View it in your browser.



Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

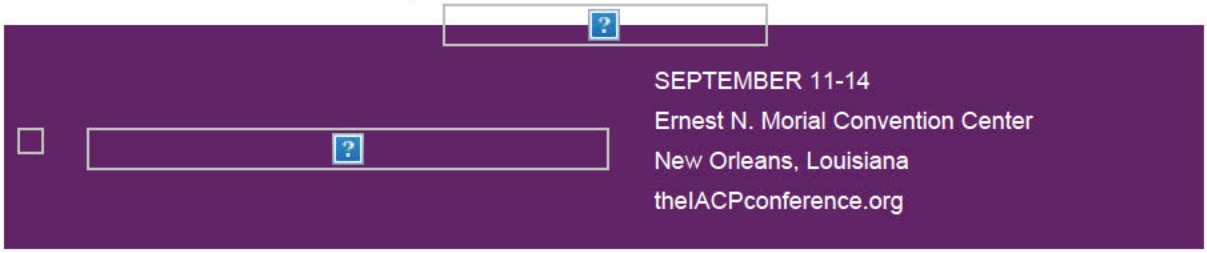
---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Rizos, Byron (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:03:16 AM

Having trouble viewing this email? View it in your browser.



Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Sonia, Michael (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 11:02:53 AM

Having trouble viewing this email? View it in your browser.

SEPTEMBER 11-14
Ernest N. Morial Convention Center
New Orleans, Louisiana
theIACPconference.org

Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: P1 Product Alert
To: Upton, Paul (POL)
Subject: Let's Connect at IACP
Date: Tuesday, August 31, 2021 12:06:04 PM

Having trouble viewing this email? View it in your browser.

SEPTEMBER 11-14
Ernest N. Morial Convention Center
New Orleans, Louisiana
theIACPconference.org

Visit us at IACP 2021 @ **Booth #3427**

to have an in-depth discussion on hot topics that include:

- **Flexible Pricing Options** to help with budget pressures, including subscription/conventional/hybrid pricing models, legacy upgrade program, and access to grant assistance partners.
- **Gold Standard Evidence Accuracy** through excellent low-light image read performance, AI-powered ALPR cameras, high-accuracy of vehicle license plate capture and hot list management.
- **Fully-configurable Data retention, sharing, auditing and reporting** to comply with local and state statutes, maintain data integrity over time, provide multi-agency interoperability and control for data sharing, and absolutely no third-party selling, merging or sharing of data by Neology.
- **Are you struggling between public protection and individual rights?** To help relieve some of the pressure, our state-of-the-art ALPR solution has cutting-edge features including windshield blurring, end-to-end evidential data with robust chain of custody, rich auditability and configurable reporting, and automatic hot list refresh with more frequent updates.

---

www.neology.net connect with us

If you do not wish to receive future Police1 Product Alerts, please unsubscribe .
To change your email address, update your profile . © 2021: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: LODD law change pending for drowned LEO; Cops gift D sney World trip to girl
Date: Wednesday, June 16, 2021 4:29:00 PM

June 16, 2021 | View as webpage

Dear Police1 Member,

Are housing costs impacting the ability of your agency to hire new officers? Have officers left your agency because they couldn't find acceptable housing?

Police1 wants to hear how the current lack of affordable housing is impacting police officers. Click here to complete our short survey. Results will be shared on Police1.

Stay safe,

— The Police1 Team

TOP STORIES

City approves petition to give drowned officer's family full pension, change law

Under Massachusetts law, drowning isn't considered a line-of-duty death, which means Officer Enmanuel Familia's wife would not get his full pension

NYPD detectives gift Disney World trip to girl who witnessed family's murder

Mass. K-9 'died a true hero' protecting officers, police say

House votes again to award Capitol Police the Congressional Gold Medal

Police: Fla. man rammed K-9 with car, broke into mayor's home

3 Honolulu police officers charged in fatal shooting

Considerations for Law Enforcement Leaders During Today's Recruitment Crisis

Law enforcement executives across the nation view recruitment and retention as a difficult challenge. While today's climate makes successful recruitment

Continue Reading

FEATURED CONTENT

Making the case for single suspect gang crime

By Nick Perna

Statutes define gang crime as involving persons committing crimes for the benefit of the gang. But what if the crime is committed by a lone wolf?



10 ways patrol officers can help the K-9 unit

By Art Carlos

Your police K-9 unit is rolling to your location to assist in locating a suspect. Follow these steps for mission success

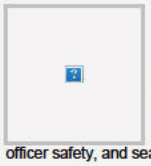


Cyberattackers are coming for public safety; prepare now

By Greg Friese, MS, NRP

Organizations and citizens have a "shared responsibility" to defend their data, computer hardware and software systems from ransomware attacks

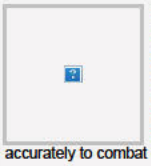
How to Start a Successful Public Safety Drone Program



The breakthrough artificial intelligence and autonomy engine built into every Skydio drone have become an irreplaceable tool for situational awareness, officer safety, and search & rescue.

Learn More

Pursue and Prevent Crime with ALPR



Jenoptik's powerful ALPR and data analysis enable you to monitor suspect vehicles and evaluate data in real time, securely and accurately to combat crime.

Learn more

OTHER HIGHLIGHTS



Would slowing down and conducting inventory have made this evidence admissible?

By Ken Wallentine



A recent case from the 4th Circuit applies the Gant rule, demonstrating its impact on a warrantless search incident to arrest



What's the best piece of advice you've received on how to stay professional?

By Police1 Staff

Every contact you make – whether on- or off-duty – leaves an impression; here are 10 ways to leave a positive, professional impression

SPONSORED CONTENT



Does your department have a rugged, reliable and versatile drone?

A drone company known for its unique coaxial technology shares how it's changing the game for drone operations in public safety.



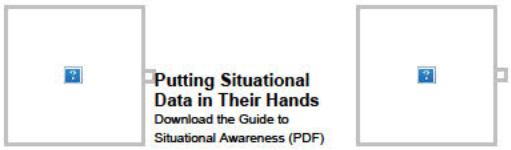
FEATURED DEAL

A Guide to Improving Officer Safety and Preparedness by

FEATURED DEAL

How To Buy Online Training Systems

Download the guide

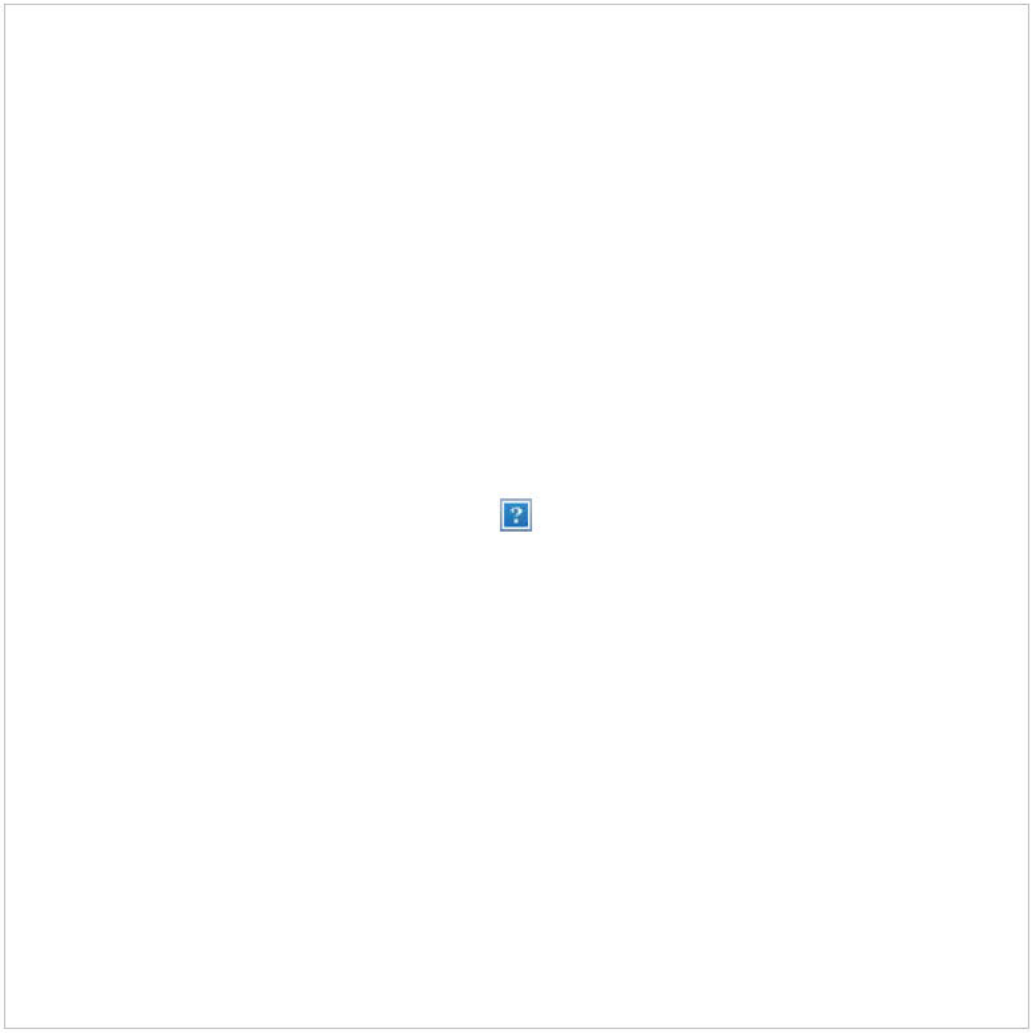


Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Harvard Law Review
To: Pinkes, William (POL)
Subject: New Issue: Volume 134 · June 2021 · Number 8
Date: Thursday, June 10, 2021 11:15:02 AM

View this email in your browser



Volume 134 · June 2021 · Number 8

ARTICLES

Policing the Emergency Room
By Ji Seon Song

In this Article, Professor Song reveals how the courts' interpretation of the Fourth and Fifth Amendments has resulted in the criminalization of the emergency room. ERs play a crucial "safety-net" function for those who do not have access to other types of medical care, yet courts have interpreted the ER as an extension of the public street, generally permitting the police to engage in highly intrusive searches and questioning. Professor Song argues that this doctrine cannot account for the unique characteristics of the ER and the medical vulnerability of patients. Moreover, Professor Song considers how police investigations in the ER are enhanced by the participation of medical professionals, who have existing professional norms as well as their own history of bias and discrimination. Finally, Professor Song shows how the courts' treatment of the ER as an extension of the street raises the same concerns of racialized policing in the ER. Professor Song then concludes by suggesting that the reasonable expectation of privacy standard should incorporate considerations of medical vulnerability and medical privacy, and that — as society questions the harm or necessity of police presence in communities — we should conceptualize ERs as patient sanctuaries to achieve a better balance between public safety and the rights of vulnerable patients.

Privacy as Privilege: The Stored Communications Act and Internet Evidence

By Rebecca Wexler

In this Article, Professor Wexler exposes a profound injustice that major technology companies have propagated through every level of the judiciary under the guise of protecting data privacy: they have leveraged the Stored Communications Act (SCA) — a key data privacy law for the Internet — to bar criminal defendants from subpoenaing the contents of another's online communications, even when those communications could exonerate the wrongfully accused. Every appellate court to rule on this issue to date has agreed with the companies. Professor Wexler argues that all these decisions are wrong as a matter of binding Supreme Court doctrine and just policy. To do this, Professor Wexler makes two novel doctrinal claims. First, she argues that when courts read the SCA to block criminal defense subpoenas, they construe the statute as creating an evidentiary privilege. Second, she argues that this construction violates a binding rule of privilege law: courts must not construe ambiguous silence in statutory text as impliedly creating a privilege because privileges are "in derogation of the search for truth." In conducting this analysis, this Article is the first to read the SCA through the lens of evidentiary privilege law, and shows how correcting the erroneous case law on this issue will enhance truth-seeking and fairness in the criminal justice system with minimal cost to privacy.

BOOK REVIEW

Making Immigration Law

By Hiroshi Motomura

In this book review, Professor Motomura begins by noting that, by building a bridge between immigration law and U.S. administrative and public law more generally, Professors Cox and Rodríguez make a major contribution in both fields, particularly through their "nuanced and persuasive" historical account of the rise of presidential power over immigration, as well as their analysis of the current relationship between Congress and the President as "co-principals" in making immigration law. However, Professor Motomura also argues that by viewing presidential immigration power as a symptom of a "structural problem" in domestic enforcement, Cox and Rodríguez do not engage fully with the international aspects of the migration-related challenges that Presidents are likely to face in the coming years and decades. As Professor Motomura puts it, events and trends outside U.S. borders — war, civil unrest, and climate change, to mention just a few — are likely in the future to influence migration to the United States even more than they do today.

Professor Motomura therefore analyzes how and why the future of presidential immigration power will most likely return to its international origins more than Cox and Rodríguez acknowledge.

NOTE

The President's Conditional Pardon Power

By the *Harvard Law Review*

The President's pardon power is considered one of the broadest powers in the Constitution. This Note identifies a dangerous potential application of that power—coercive conditional pardons. Fortunately, as this Note argues, English common law, American founding, and Supreme Court precedent all indicate the President may not grant pardons on whatever conditions he or she chooses, but for that reason, understanding the limits of the President's conditional pardon power requires a fresh look at the pardon power's theoretical underpinnings and historical practice.

RECENT CASES

United States v. Jones

By the *Harvard Law Review*

In *United States v. Jones*, the Seventh Circuit vacated a district court's seventy-year sentence that was more than double the Sentencing Guidelines' recommended sentencing range on the grounds that the district court did not sufficiently justify it. However, the author argues that the panel also paved the way for the district court to impose the same sentence on remand by suggesting justifications. The author argues that this exemplifies how the post-*Booker* federal sentencing scheme gives district courts broad sentencing discretion accompanied by perfunctory, formalistic appellate review, making sentencing outcomes vary according to luck of the judicial draw.

Otto v. City of Boca Raton

By the *Harvard Law Review*

In *Otto v. City of Boca Raton*, the Eleventh Circuit held that bans against minor conversion therapy violated the First Amendment. The author argues that in doing so, the court incorrectly categorized talk therapy as constitutionally protected speech, rather than regulable speech incidental to professional conduct. With a fresh circuit split and ongoing courtroom battles, the constitutionality of conversion therapy bans may soon reach the Supreme Court.

Revitch v. DIRECTV, LLC

By the *Harvard Law Review*

Emboldened by decades of pro-arbitration decisions from the Supreme Court, corporations are drafting arbitration agreements with increasingly "infinite" terms — terms that purport to bind consumers to arbitrate all disputes that might arise not only with the company itself, but with a wide range of affiliated and related entities. Recently, in *Revitch v. DIRECTV, LLC*, the Ninth Circuit rejected DirecTV's attempt to compel arbitration on the basis of a contract a consumer had signed with AT&T years before AT&T's parent company had purchased DirecTV. The author argues that, while the result was heartening, the court's reasoning contained several fatal weaknesses, although a separate concurrence introduced a novel theory that may support broad-based judicial rejection of these abusive contracts.

United States v. Trice

By the *Harvard Law Review*

In *United States v. Trice*, the Sixth Circuit held that the area surrounding a tenant's apartment does not count as curtilage under the Fourth Amendment. The author argues that this decision failed to extend the same Fourth Amendment protections enjoyed in suburbia to the context of low-rent apartment buildings. In doing so, the Sixth Circuit contributed to exacerbating the racial, ethnic, and class inequalities that exist under current Fourth Amendment jurisprudence.

Commonwealth v. McCarthy

By the *Harvard Law Review*

In *Commonwealth v. McCarthy*, the Massachusetts Supreme Judicial Court held that the use of automated license plate readers (ALPRs) may constitute a search, though it did not in this instance. The author argues that future courts should treat ALPR usage with greater scrutiny. ALPR data can be maintained for potentially indefinite durations; in opaque,public-private databases, lacking in privacy protections; and the tools reveal a scale of information unavailable to law enforcement through traditional surveillance techniques.

FORUM & BLOG

The *Harvard Law Review Forum* is publishing four exciting pieces in the month of June. Two are Responses to recently published articles, one is a Reflection on sexual harassment in the federal judiciary, and one is an Essay on caste discrimination. The Blog will continue to post editor-authored case comments and pieces by outside authors on recent legal developments.

Beware of Giant Tech Companies Bearing Jurisprudential Gifts

By Kiel Brennan-Marquez

In *Privacy as Privilege*, Professor Rebecca Wexler argues that courts should stop construing the Stored Communications Act (SCA) to block criminal defense–side subpoenas for communication records. In this Response, Professor Brennan-Marquez tells what he calls a more important story, one that originates from the same facts and also features disadvantaged criminal defendants, but in which those defendants are not the main characters. Rather, the main characters are the giant tech companies that have routinely been served with defense subpoenas (under the SCA), appeared in court to contest those subpoenas, and won — securing "privacy victories" for their users. According to Professor Brennan-Marquez, the moral of the story, boiled down, is that we should beware of these victories; for they are not quite what they appear, and that a system in which the boundaries of communication privacy are negotiated at the behest of the very entities whose profit model relies on their erosion is not a healthy one.

Enough Is Not Enough: Reflection on Sexual Harassment in the Federal Judiciary

By Olivia Warren

This Reflection shares Ms. Warren's powerful firsthand experience with sexual harassment while clerking for the late Judge Reinhardt. Building on testimony that she shared before Congress on the matter, Warren describes the painful differences between what she had hoped for in working for Judge Reinhardt and the reality of being relentlessly sexually harassed and verbally attacked for a year. While her story details the renewed sense of confidence that she has gained in reclaiming her story and speaking out, it also names the many continuing ways in which the judiciary, Harvard Law School, and the legal profession enable the perpetuation sex- and gender-based violence. Warren concludes the piece by noting the persisting contrast between these two lessons, writing that

"there is virtue in screaming into the face of deafening indifference, if only because the sound of my voice reminds me that I have not yet succumbed to it.".

Title VII and Caste Discrimination

By Guha Krishnamurthi & Charanya Krishnaswami

In their Essay, Krishnamurthi and Krishnaswami argue that caste discrimination — which has grown rapidly in the technology and engineering sectors in particular — is covered by Title VII of the Civil Rights Act of 1964. In Part I of the piece, they explain the basic contours and characteristics of the South Asian caste system and detail the reach and impact of caste in the United States. In Part II, they explain how caste discrimination is, as a legal matter, cognizable under Title VII as discrimination based on "race," "religion," or "national origin," following the Supreme Court's decision in Bostock v. Clayton County, in which the Court found that sexual orientation discrimination is a type of sex discrimination. The authors then briefly conclude by contending that despite the coverage of caste discrimination under federal law, either the U.S. Equal Employment Opportunity Commission (EEOC) or Congress should provide further clear guidance — and in doing so, should consider other kinds of discrimination throughout the world that should be explicitly prohibited in the United States.

Abortion as an Instrument of Eugenics

By Michael Stokes Paulsen

This Response takes a critical lens to Professor Murray's *Race-ing Roe* and argues that trait-selection abortion bans undermine the logic of *Roe v. Wade* in ways that Professor Murray does not address. First, the piece argues that if it is wrong to have an abortion in order to select against a certain trait (e.g., sex or disability status), then this may reveal that it is wrong to have an abortion, full stop. Second, the Response joins Justice Thomas in understanding the history and contemporary practice of abortion to create a racial disparate impact, thus making abortion an instrument of eugenics even if there exists no widespread eugenicist conspiracy around abortion access. Lastly, the piece argues that trait-selective abortion ought to be understood as unconstitutional, and that stare decisis ought not prevent the Supreme Court from overturning Roe's central holding.

Copyright © 2021 Harvard Law Review, All rights reserved.
You are receiving this email because you signed up at our website.

Our mailing address is:
Harvard Law Review
Gannett House
1511 Massachusetts Ave
Cambridge, MA 02138

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list

From: Police1 Roll Call
To: Cooper, Brian (POL)
Subject: No more thin blue line patches for PD; LEO®s Olympic journey
Date: Thursday, August 12, 2021 6:11:38 PM

August 12, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES

‘I missed my job’: Olympic hurdler returns to police work after Tokyo Games

When she’s not chasing Olympic glory, Mulern Jean works as a school resource officer in South Carolina

NY bill that would have let police sue protesters is vetoed

Philly PD hit with contempt motions over not sharing misconduct data

San Diego-area police academy classes suspended over COVID cases

Ill. board votes to remove ‘thin blue line’ patches from police uniforms

Austin city leaders balk at $119M annual price tag of police ballot measure

Pair Your Wireless Earphones to your Radio

Air Pro Wireless Adapter lets you use your favorite earphones, like Apple Airpods, with your 2-way radio.

Shop adapters

Rekor Finder: Powerful & Discrete in-vehicle ALPR

Finder is a cost-effective, in-vehicle ALPR solution that accurately identifies license plates and vehicles in real-time at high speeds and extreme angles.

Learn more

FEATURED CONTENT

State your case: Should law enforcement agencies use unmarked vehicles for traffic enforcement?

By Jim Dudley and Chief Joel Shults, EdD
Despite fewer cars on the road due to COVID-related shutdowns, the national trend has been higher incidents of speeding and fatalities

Detention of man with AR-15 walking toward school was lawful

By Ken Wallen ine

The court noted that, given the mass murder at Marjory Stoneman Douglas High School, "any reasonable officer [would] be on heightened alert for copycat crimes"

Finally, Law Enforcement Technology for Everybody

Arrest to Adjudication: Agisent Technologies provides integrated solutions for agencies, prosecutors, and state-wide investigators: RMS ONE, PlatformRMS, ProDocs, ProCase, and Fusion Centers.

Grants, subsidies, and free-trials

Predict Criminal Patterns With ALPR

Learn how powerful ALPR cameras combined with advanced analysis software allow law enforcement to identify and predict suspect behaviors enabling them to effectively pursue and prevent crime.

Find out more

COLLEGE DEGREES IN LE

Opinion: Why the next generation of cops need a criminal justice degree

By Janay Gasparini, Ph.D.

Forging partnerships with faculty members at local colleges and universities can have a direct impact on the quality of officer candidates in your region

Why you should stop listening to the critics and go earn your college degree

By Marcus Rinaldi

A college education plays an important role in developing the interpersonal skills and

critical thinking required as a law enforcement officer

SPONSORED CONTENT

Does your department have a rugged, reliable and versatile drone?

A drone company known for its unique coaxial technology shares how it's changing the game for drone operations in public safety.

FEATURED RESOURCES

How to buy jail management software

Get the guide

FEATURED EDUCATION

Online M.S. in LE Leadership

Start your master's degree this year. Top-ranked program, 100% online.

FEATURED COMPANY NEWS

Estes AWS introduces 2021 Tahoe mounting solution

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

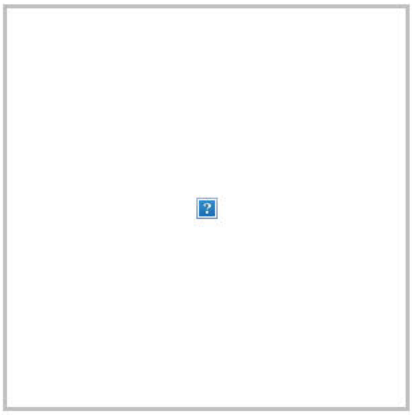
If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lawlor Jr, Daniel (POL)
Subject: No more thin blue line patches for PD; LEO®s Olympic journey
Date: Thursday, August 12, 2021 6:12:05 PM

August 12, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



‘I missed my job’: Olympic hurdler returns to police work after Tokyo Games

When she’s not chasing Olympic glory, Mulern Jean works as a school resource officer in South Carolina

NY bill that would have let police sue protesters is vetoed

Philly PD hit with contempt motions over not sharing misconduct data

San Diego-area police academy classes suspended over COVID cases

Ill. board votes to remove ‘thin blue line’ patches from police uniforms

Austin city leaders balk at $119M annual price tag of police ballot measure

Pair Your Wireless Earphones to your Radio

Air Pro Wireless Adapter lets you use your favorite earphones, like Apple Airpods, with your 2-way radio.

Shop adapters

Rekor Finder: Powerful & Discrete in-vehicle ALPR

Finder is a cost-effective, in-vehicle ALPR solution that accurately identifies license plates and vehicles in real-time at high speeds and extreme angles.

Learn more

FEATURED CONTENT

State your case: Should law enforcement agencies use unmarked vehicles for traffic enforcement?

By Jim Dudley and Chief Joel Shults, EdD
Despite fewer cars on the road due to COVID-related shutdowns, the national trend has been higher incidents of speeding and fatalities

Detention of man with AR-15 walking toward school was lawful

By Ken Wallen ine

The court noted that, given the mass murder at Marjory Stoneman Douglas High School, "any reasonable officer [would] be on heightened alert for copycat crimes"

Finally, Law Enforcement Technology for Everybody

Arrest to Adjudication: Agisent Technologies provides integrated solutions for agencies, prosecutors, and state-wide investigators: RMS ONE, PlatformRMS, ProDocs, ProCase, and Fusion Centers.

Grants, subsidies, and free-trials

Predict Criminal Patterns With ALPR

Learn how powerful ALPR cameras combined with advanced analysis software allow law enforcement to identify and predict suspect behaviors enabling them to effectively pursue and prevent crime.

Find out more

COLLEGE DEGREES IN LE

Opinion: Why the next generation of cops need a criminal justice degree

By Janay Gasparini, Ph.D.

Forging partnerships with faculty members at local colleges and universities can have a direct impact on the quality of officer candidates in your region

Why you should stop listening to the critics and go earn your college degree

By Marcus Rinaldi

A college education plays an important role in developing the interpersonal skills and

critical thinking required as a law enforcement officer

SPONSORED CONTENT

Does your department have a rugged, reliable and versatile drone?

A drone company known for its unique coaxial technology shares how it's changing the game for drone operations in public safety.

FEATURED RESOURCES

How to buy jail management software

Get the guide

FEATURED EDUCATION

Online M.S. in LE Leadership

Start your master's degree this year. Top-ranked program, 100% online.

FEATURED COMPANY NEWS

Estes AWS introduces 2021 Tahoe mounting solution

Police1 does not send unsolicted messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: ASIS International
To: Upton, Paul (POL)
Subject: Open Forum Digest for Monday July 12, 2021
Date: Tuesday, July 13, 2021 1:57:54 AM

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

Open Forum

Post New Message

Jul 12, 2021

Discussions

started 8 hours ago, Paul Sprague (0 replies)

Guard Tour Patrol System

1. Researching Guard Tour Patrol Systems. Have read... Paul Sprague

started 17 hours ago, William Reed (0 replies)

Podcast Guest Request

2. Hello all, I co-host a security-related... William Reed

started yesterday, Charles Andrews CPP (1 reply)

ISC West 2021, who is attending?

3. Ameristar Perimeter Security will be attending.... Bret Villars PSP

started 4 days ago, Scott Napier PSP (9 replies)

Paperless post orders and SOP's?

4. Hi Scott, I would analyze this through the... Eric Lee PCI, PSP
5. @John Lepant APP < Andrew Saluke

started 5 days ago, John Overacker (14 replies)

Cloud Based Video Surveillance

6. Hey John, From your signature, I am guessing... Eric Lee PCI, PSP
7. @John Overacker < Andrew Saluke
8. John, I also want to publicly thank @Andrew... Jon Polly PSP

started one month ago, Gayle Rosnick (3 replies)

How the POA Revisions Affect Those S\studying for an ASIS Exam

9. Hi Harmeet, I recently completed the CPP exam... Eric Lee PCI, PSP

10. Thanks to all for your input and updates in... Larry Breland

top next

1. Guard Tour Patrol System

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 4:34 PM
Paul Sprague

Researching Guard Tour Patrol Systems. Have read a lot of posts. Have also gone to a lot of sites looking for information. Have found the ones I have looked at, have too many Bells And Whistles. We are a resort, couple dozen buildings, 24/7 Security. We are also in a mountain community. Have one area. We are not spread all over the place, only a proprietary security team. Our current Watchman system is old and outdated. Looking to keep up with the technology. Have any ideas. TIA

Paul Sprague
Security Director
Winter Park Resort
Winter Park CO
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

top previous next

2. Podcast Guest Request

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 7:22 AM

William Reed

Hello all,
I co-host a security-related podcast called The Coffee Squad Podcast. I would like to invite anyone who might be interested to join us to share your stories and expertise in the security field. Please contact me with any questions or to schedule your episode! The Coffee Squad Podcast - Security Matters

Coffeesquadpodcast

The Coffee Squad Podcast - Security Matters

Talking the State of Policing with a Police Chief - June 21, 2021 Home Security Systems: What is best for you? - June 14, 2021 Managing Violence with Joe Saunders - June 7, 2021

View this on Coffeesquadpodcast ≥

William Reed
Associate Director of Security Training
Freedom Consulting LLC
william@fc-llc.org
Hampstead NC
United States

Reply to Group Online View Thread Like Forward

Flag as Inappropriate

top previous next

3. Re: ISC West 2021, who is attending?

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 9:04 AM
Bret Villars PSP

Ameristar Perimeter Security will be attending. I look forward to meeting you and discussing our solutions for Perimeter and high Security applications (including fencing, bollards, barriers, anti-crash, ant-climb, etc...).

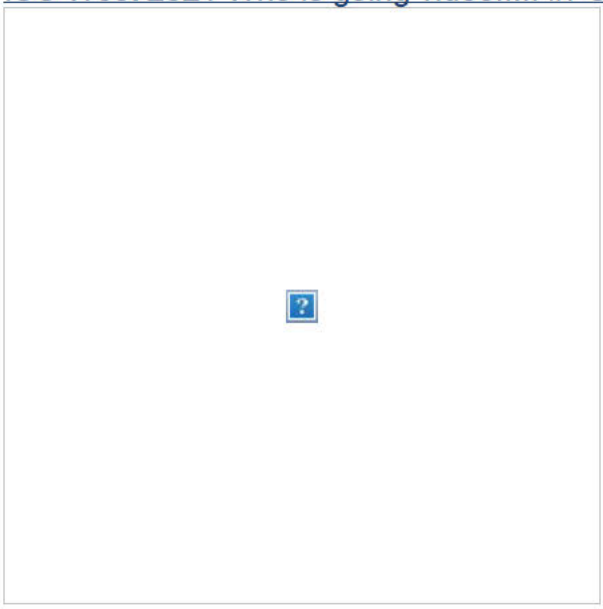
Bret Villars PSP
National Business Development US & Canada
AssaAbloy Ameristar
Mandeville LA
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 11 Jul, 2021 14:33
From: Charles Andrews
Subject: ISC West 2021, who is attending?

CLICK HERE FOR Video..
ISC West 2021 Who is going video..... #FOC



Charles Andrews CPP
Chairman of the Board & Founder
Friends of Chuck (FOC)
Lake Jackson TX
United States
---

top previous next

4. Re: Paperless post orders and SOP's?

Reply to Group via Email | Reply to Sender Online



Jul 12, 2021 3:10 AM
Eric Lee PCI, PSP

Hi Scott,

I would analyze this through the fundamental AIC of infosec, and compare it to your business' needs. For those who are comfortable and familiar with computers, a digital SOP can be very beneficial by providing multiple indexing, better flow through links and at minimum being able to leverage simple search features.

Can you ensure the availability, integrity and confidentiality of the SOP to ensure continuous operation and whether the benefits outweigh the risk?

Challenges would be based on work environment and staffing. Are your staffing all comfortable in accessing the information? Will the information be accessible in a power or network outage and what are the likelihood of needing the information in those instances.

I had issues when my management team moved our SOPs to completely digital because of these issues. Power outage SOP and checklists were digitized without hardcopy back up and our guard population was not all comfortable.

I think it largely depends training provided and how the SOPs are used. I wouldn't really be comfortable having crisis management SOPs or checklists strictly on a digital platform, but for day to day activity where SOP that have less urgency, I think there are benefits.

Based on Zendesk being a software company, I'm sure your staff have no issues with digitized and your system continuity is robust enough that there should be minimal risk. Also, I would also assume that if there is a power or network outage your team wouldn't be able to do anything even if you had access to the SOPs.

Eric Lee PCI, PSP
Security Supervisor
Russell Security Services Inc
Everett ON
Canada

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:

Sent: 08 Jul, 2021 13:05
From: Scott Napier
Subject: Paperless post orders and SOP's?

Looking for some feedback on having paperless post orders and SOP's/ Playbooks for your ECP's, control rooms and GSOC type spaces. By paperless I mean a shared drive where everyone who needs them has quick access, but there is no actual hard copy at each location.

Scott Napier PSP
Global Safety and Security
Systems and Technology Lead
Zendesk
United States
---

top previous next

5. Re: Paperless post orders and SOP's?

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 9:36 AM
Andrew Saluke

@John Lepant APP definitely a good idea to have paper copies, especially for a power outage contingency. Most of the time the computer systems have power, but of course service disruptions do happen.

You raise a great point in your 'what's the harm' question. For the security teams I've encountered who want the digital SOPs, they are seeking to: 1) ensure everyone is operating off the most updated playbook; 2) respond faster and according to plan; 3) track whether & how quickly team members are following the plan.

Regards,
Andrew

Andrew Saluke

Topo.ai
andrew.saluke@topo.ai
Alpharetta, GA

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 10 Jul, 2021 12:19
From: John Lepant
Subject: Paperless post orders and SOP's?

What is the Plan if there is a power outage or the computer crashes? What is the harm of having paper copies? Can you keep it secure from hackers?

If you have paper copies they can serve when the computers are down.

John Lepant APP
Security Professional
Allied Universal
Brighton CO
United States

top previous next

6. Re: Cloud Based Video Surveillance

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 3:21 AM
Eric Lee PCI, PSP

Hey John,

From your signature, I am guessing you work for a municipal government. Before even exploring cloud options, I would suggest checking with legal counsel to see if the benefits are worthwhile. Privacy, retention and service provider cybersecurity standards for government agencies may not make it feasible to use cloud storage

solutions.

Eric Lee PCI, PSP
Security Supervisor
Russell Security Services Inc
Everett ON
Canada

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 07 Jul, 2021 14:13
From: John Overacker
Subject: Cloud Based Video Surveillance

Hello Everyone,

Looking to get input from end-users on cloud-based video surveillance. We are currently looking into phasing out our coax-based cameras and DVR to a cloud-hosted solution. A few years ago we ran Ethernet (PoE) to the locations of all of our current cameras so we would like to find something that is relatively plug and play that we can do in-house. We do have multiple sites that are not all on the same computer network.

We would be interested in a service that could offer people counting, analytics, etc.

If anyone has any suggestions on vendors to check out or personal experiences, please let me know.

Thanks.

John Overacker
Director of Safety and Security
Town of Perinton
Fairport, New York
585-223-0770
---

7. Re: Cloud Based Video Surveillance

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 9:40 AM
Andrew Saluke

@John Overacker you may wish to chat with @Jon Polly PSP. He is knowledgeable on 'smart city' use cases and may be able to help you identify some good options that account for present and future needs.

Good luck!

Andrew

Andrew Saluke
Topo.ai
andrew.saluke@topo.ai
Alpharetta, GA

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 07 Jul, 2021 14:13
From: John Overacker
Subject: Cloud Based Video Surveillance

Hello Everyone,

Looking to get input from end-users on cloud-based video surveillance. We are currently looking into phasing out our coax-based cameras and DVR to a cloud-hosted solution. A few years ago we ran Ethernet (PoE) to the locations of all of our current cameras so we would like to find something that is relatively plug and play that we can do in-house. We do have multiple sites that are not all on the same computer network.

We would be interested in a service that could offer people counting, analytics, etc.

If anyone has any suggestions on vendors to check out or personal experiences,

please let me know.

Thanks.

John Overacker
Director of Safety and Security
Town of Perinton
Fairport, New York
585-223-0770
---

top previous next

8. Re: Cloud Based Video Surveillance

Reply to Group via Email | Reply to Sender Online



Jul 12, 2021 12:39 PM
Jon Polly PSP

John,

I also want to publicly thank @Andrew Saluke for his recommendation.

I would echo many of the statements already mentioned here. If I may, there are a few things that must be addressed from a public safety perspective.

1) All city-owned public safety video typically has a requirement for the recording to be Criminal Justice Information Services (CJIS) compliant if it is to be used in court as evidence. This is where NOT all cloud providers are the same. The reason most police departments choose to use on-premise solutions instead of cloud is that finding a CJIS compliant cloud application is rare. Many cloud VMS providers are using AWS cloud, which is not CJIS compliant. AWS Government and Azure Government are CJIS compliant, but there is a cost difference.

2) What is the retention time and expected use of the video? As many cities have found with body-worn camera video, the cost of long-term storage (over 1 year) gets to be very expensive. Video is very large and when storing in the cloud it can get very expensive quickly to record long term. Not saying it is not worth having the OPEX vs CAPEX option to have a Video Surveillance as a Service (VSaaS) option;

merely something to consider. If the video is of a homicide with lifetime retention, that one video may become very expensive over time.

3) As it was mentioned earlier, the resolution in what the video was recorded is important. Many cloud providers have a limitation of 1080P (2 Megapixel) video. If the city chooses to install 4, 5, 8MP (4K) cameras, the recording may be "dumbed down" depending on the cloud provider to keep costs and storage down. Is this acceptable?

4) I know it was mentioned earlier, but I would re-iterate that any system has an open architecture, simply because cities have multiple data sources they need to access that Corporate, Commercial, or Schools do not. The ability to ingest analytics from 3rd parties, video through Public-Public and Public-Private Partnerships (P3s), or federal databases such as the FBI's National Crime Information Center (NCIC) and Department of Motor Vehicle (DMV). Automated License Plate Recognition (ALPR) that are typically installed, when connected to NCIC, can provide data and increase officer awareness and officer safety.

5) Who in the city is going to manage the cloud application? I ask this since "cloud" is simply someone else's data center. Depending on the city, this may fall to IT, Police IT, or the Criminal Intelligence Unit (CIU). Again, this is a question of how the system gets used, not necessarily the medium where it is recorded.

There are pros and cons for cloud recording options, just as there are for on-premise and hybrid solutions.

You also mention the analytics piece, and I do not want to just gloss over this. Again, there is not a simple answer here. Most top-tier cameras have built-in edge analytics. Most are AI-enabled analytics somewhere on the continuum. I think AI-enabled analytics is best described by IBM Program Manager Eda Kavlakoglu, when she proposed AI as a Russian nesting doll. AI is the large container, the next doll is Machine Learning, then Neural Networks, and last the Deep Learning doll. Edge analytics are being offered three ways today; on the camera, co-located edge appliance, or cloud (both proprietary and non-proprietary options). Some analytics quite simply take too much compute (even as cameras become bigger powerhouses) and must be server or cloud-based. Depending on where the cameras are being used, either directly connected or via wireless or cellular options may determine what analytics can be used, due to bandwidth or data package restraints.

I hope these points resonate and please feel free to reach out if you would like.

Thank you,
Jon

Jon Polly, PSP, IC3PM
Chief Solutions Officer
Protecht Solutions Partners, LLC
(704) 759-6837
Charleston SC
United States
www.protechtsolutionspartners.com

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 07 Jul, 2021 14:13
From: John Overacker
Subject: Cloud Based Video Surveillance

Hello Everyone,

Looking to get input from end-users on cloud-based video surveillance. We are currently looking into phasing out our coax-based cameras and DVR to a cloud-hosted solution. A few years ago we ran Ethernet (PoE) to the locations of all of our current cameras so we would like to find something that is relatively plug and play that we can do in-house. We do have multiple sites that are not all on the same computer network.

We would be interested in a service that could offer people counting, analytics, etc.

If anyone has any suggestions on vendors to check out or personal experiences, please let me know.

Thanks.

John Overacker
Director of Safety and Security
Town of Perinton
Fairport, New York
585-223-0770
---

9. Re: How the POA Revisions Affect Those S\studying for an ASIS Exam

Reply to Group via Email | Reply to Sender Online



Jul 12, 2021 2:52 AM
Eric Lee PCI, PSP

Hi Harmeet,

I recently completed the CPP exam, July 6, and there are still 7 domains on exam.

According to the certification handbook, "In 2019/2020, ASIS conducted a job analysis study to ensure the CPP Body of Knowledge still represents the knowledge and skills needed to be a successful security manager...Exam questions regarding the new information will start to appear on the exam in early 2021." Also it shows that the Information Security domain has gone from 9% to 14%, so I don't see it going away despite not having a corresponding POA book.

I had previously reviewed some online resources for SSCP and CISSP and found that the information was consistent with the CPP Study Guide.

The study guide was the only formal resource that I used for the CPP because I just also recently completed the PSP and PCI. I haven't read the POA, neither the 2021 edition or prior, but was comfortable doing the exam from studying the contents in the PSP and PCI texts.

Eric Lee PCI, PSP
Security Supervisor
Russell Security Services Inc
Everett ON
Canada

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 11 Jul, 2021 07:37
From: Harmeet Singh Kapoor

Subject: How the POA Revisions Affect Those S\studying for an ASIS Exam

Seeking a clarification w.r.t study material for CPP.
Which study material is recommended for CPP exam preparation- *Protection of Assets (2021 edition) Bundle OR *ASIS Certified Protection Professional (CPP®) Study Manual (The) (Softcover).
It may please be noted that ASIS Certified Protection Professional (CPP®) Study Manual (The) (Softcover) has SEVEN domains. Whereas, Protection of Assets (2021 edition) Bundle comprises of only six books and does not cover one domain. Hence the confusion.

Kindly clarify.

Harmeet Singh Kapoor
Lt Col
Government
Mohali
India

top previous

10. Re: How the POA Revisions Affect Those S\studying for an ASIS Exam

Reply to Group via Email | Reply to Sender Online

Jul 12, 2021 3:37 PM
Larry Breland

Thanks to all for your input and updates in regards to the ASIS Exam. I have been studying for the CPP Exam using the flash cards and it is a lot of information to retain. For those who have successfully obtain their certification any advice on study habits would be greatly appreciated.

Larry Breland
Executive Protection Agent
Self-Employed
CLARKSVILLE TN
United States

Reply to Group Online View Thread Like Forward

Flag as Inappropriate

Original Message:
Sent: 09 Jun, 2021 12:38
From: Gayle Rosnick
Subject: How the POA Revisions Affect Those S\studying for an ASIS Exam

Hello all!

We have seen many posts about people studying for an ASIS certification exam and worried about the release of the updated POA. But don't worry! None of the current exam questions are being changed! Please remember that you are being tested on the exam's body of knowledge; not on the POA or the other recommended reading materials. Our exams are testing your understanding of the concepts of security management principles, which are explained in our reference materials.

Right now, we have a group of 30+ subject matter experts reviewing all the live exam questions on our four exams. They will take existing test questions and re-reference them to the new POA version. If a test question cannot be re-referenced to the new version, that item will be retired and will not appear on the exam.

As ASIS volunteers write new items, they will be referenced to the new version but the new questions will be pre-tested on future exams as unscoreable. This allows ASIS to determine if the new question is performing correctly in the field. Only when the item's performance is deemed appropriate is it finally made "scoreable" on future forms. This entire process takes about a year, from the time the new reference is published to when there are new scoreable items on the exam. Please click here for information on the new volumes of the POA.

Please feel free to contact the Certification Team at certification@asisonline.org if you have additional questions.

Gayle Rosnick
Director, Certification
ASIS International
Alexandria VA
United States

You are subscribed to "Open Forum" as paul.upton@pol.state.ma.us. To change your subscriptions, go to My Subscriptions. To unsubscribe from this community discussion, go to Unsubscribe.

From: ASIS International
To: Upton, Paul (POL)
Subject: Open Forum Digest for Wednesday May 12, 2021
Date: Thursday, May 13, 2021 2:04:00 AM

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

Open Forum

Post New Message

May 12, 2021

Discussions

started 6 hours ago, Calvin Yadav (0 replies)

FREE Invitation: Leading Ethical AI in Video Analytics

1. I wanted to #invite everyone in this group on... Calvin Yadav

started 9 hours ago, James Hamrick (0 replies)

Whitepaper - Transforming Public Safety through Blockchain Technology

2. Good afternoon, colleagues, From a discussion... James Hamrick

started 13 hours ago, Eugene Posey (3 replies)

Simple easy to use CAD-like software or program

3. Greetings all, I'm looking for a simple easy... Eugene Posey
4. Hello Eugene, You could look into BlueBeam... Bobby Cannon PSP
5. Hi Eugene, I agree with Bobby - Bluebeam is a... Roy Parks CPP, PSP
6. Another vote for BlueBeam. It's a great tool... Dusan Losic CPP, PSP

started yesterday, Dallin Law PSP (3 replies)

Video Surveillance Case Law

7. Dallin, I am NOT an attorney; however, I found... L. Lanark Lockard
8. Thanks, L, this is useful information I have... Dallin Law PSP
9. Dallin, I don't have the case law, and I am... Jon Polly PSP

started 2 days ago, Suzanne Altimore (4 replies)

CPP Study Groups for Exam Review

10. Hi Mike / Hi Suzanne, Robert Natoli from the... Roy Parks CPP, PSP

started 2 days ago, Joseph Gwei PSP (5 replies)

Passed the CPP Certification Exam

11. Awesome. Congratulations Dinesh Mohanaraj

top next

1. FREE Invitation: Leading Ethical AI in Video Analytics

Reply to Group via Email | Reply to Sender Online

May 12, 2021 6:35 PM | view attached

Calvin Yadav

I wanted to #invite everyone in this group on MAY 13, to elevate the #conversation on #Ethicalai and how we can use the #AI to create a #safer and #smarter world. **#artificialintelligence #innovation #machinelearning #iot #analytics #ml #deeplearning #bigdata**

www.eventbrite.com/e/...

Calvin Yadav
CEO
IREX
Murrieta CA
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

top previous next

2. Whitepaper - Transforming Public Safety through Blockchain Technology

Reply to Group | Reply to Sender

via Email | Online

May 12, 2021 3:41 PM | view attached

James Hamrick

Good afternoon, colleagues,

From a discussion we were having in the Information Technology Security Community on supply chain security, I was asked to share a whitepaper I had written a few months ago on how blockchain technology could potentially transform public safety and the criminal justice system.

I have attached my whitepaper, and would appreciate any feedback.

Thanks!

James Hamrick, Security+
IT Technical Support Specialist & Facility Security Officer
IBM Corporation
Annapolis Junction, MD
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

top previous next

3. Simple easy to use CAD-like software or program

Reply to Group via Email | Reply to Sender Online

May 12, 2021 10:56 AM
Eugene Posey

Greetings all,

I'm looking for a simple easy to use CAD-like software or program I can use to

create an event footprint or sitemap/grid referencing system to allow for rapid identification of event-specific markers and emergency locations such as First aid, Information, Security, Entrance/Exit, etc.

Eugene Posey
CEO/Operations Manager
Greenroom Security Agency, LLC.
Chicago IL
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

top previous next

4. Re: Simple easy to use CAD-like software or program

Reply to Group via Email | Reply to Sender Online



May 12, 2021 12:04 PM
Bobby Cannon PSP

Hello Eugene,

You could look into BlueBeam Revu. It's a PDF editor software you can also use to mark up blueprints, and has various tools / icons for download and usage. Not sure on price point, but its also useful on collaboration.
www.bluebeam.com/solutions/revu

Bobby Cannon PSP
Equinix
Flowery Branch GA
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 12 May, 2021 10:56
From: Eugene Posey
Subject: Simple easy to use CAD-like software or program

Greetings all,

I'm looking for a simple easy to use CAD-like software or program I can use to create an event footprint or sitemap/grid referencing system to allow for rapid identification of event-specific markers and emergency locations such as First aid, Information, Security, Entrance/Exit, etc.

Eugene Posey
CEO/Operations Manager
Greenroom Security Agency, LLC.
Chicago IL
United States
---

top previous next

5. Re: Simple easy to use CAD-like software or program

Reply to Group via Email | Reply to Sender Online

May 12, 2021 1:27 PM
Roy Parks CPP, PSP

Hi Eugene,

I agree with Bobby - Bluebeam is a powerful tool that is easy to use for marking up static floor plan drawings in PDF format. I use it daily when I don't need to use AutoCAD (not simple to learn & expensive). Bluebeam has a 30-day trial period so you can see if it works for you before you buy.

Best!

Roy Parks CPP, PSP

Senior Manager
Kroll, a division of Duff & Phelps
Broadlands VA
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 12 May, 2021 12:03
From: Bobby Cannon
Subject: Simple easy to use CAD-like software or program

Hello Eugene,

You could look into BlueBeam Revu. It's a PDF editor software you can also use to mark up blueprints, and has various tools / icons for download and usage. Not sure on price point, but its also useful on collaboration.
www.bluebeam.com/solutions/revu

Bobby Cannon PSP
Equinix
Flowery Branch GA
United States

top previous next

6. Re: Simple easy to use CAD-like software or program

Reply to Group via Email | Reply to Sender Online

May 12, 2021 11:30 PM
Dusan Losic CPP, PSP

Another vote for BlueBeam. It's a great tool and very easy to use. Microsoft Visio is another option to consider, particularly if you need anything more diagrammatic, flowcharts, etc. Steeper learning curve and not as intuitive. I use both on a regular basis.

Dusan Losic CPP, PSP
www.securityconsultant.net

Reply to Group Online View Thread Like Forward

Flag as Inappropriate

Original Message:
Sent: 12 May, 2021 10:56
From: Eugene Posey
Subject: Simple easy to use CAD-like software or program

Greetings all,

I'm looking for a simple easy to use CAD-like software or program I can use to create an event footprint or sitemap/grid referencing system to allow for rapid identification of event-specific markers and emergency locations such as First aid, Information, Security, Entrance/Exit, etc.

Eugene Posey
CEO/Operations Manager
Greenroom Security Agency, LLC.
Chicago IL
United States
---

top previous next

7. Re: Video Surveillance Case Law

Reply to Group via Email Reply to Sender Online

May 12, 2021 4:13 AM
L. Lanark Lockard

Dallin,
I am NOT an attorney; however, I found a case in the 9th US Circuit Court of

Appeals that indicates there are some expectations of privacy regarding being tracked through facial recognition by private organizations (non-law enforcement), in this case it was Facebook. A Federal Court Sounds the Alarm on the Privacy Harms of Face Recognition Technology | American Civil Liberties Union (aclu.org). I would recommend you contact your general counsel at Utah State University. This is an unsettled area of law and may differ in other US Circuit Courts and State Appellate or Supreme Courts.

L. Lanark Lockard
Specail Agent (retired)
Retired from Naval Criminal Investivative Service
Kailua HI
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 11 May, 2021 17:39
From: Dallin Law
Subject: Video Surveillance Case Law

Does anyone have a resource or a list of Case Law or Jurisprudence in regards to video surveillance systems use? Most particularly in places of higher education.

We are having issues with identifying the unknowns in the way of should we have facial recognition. What does that do to the image of the Higher education institution?

Should we record license plates can these be used in a court of law. If so what legal requirements must be met in order to have strong evidence for the purpose of the trial? Can we be held culpable if we have certain capabilities but not utilize them?

I'm looking for case law or lessons learned in this area so we can apply policies and procedures and deploy technology appropriately to protect ourselves and students/guests.

Dallin Law, PSP
Physical Security Professional
Utah State University

Logan, Utah
USA
---

top previous next

8. Re: Video Surveillance Case Law

Reply to Group via Email | Reply to Sender Online

May 12, 2021 10:26 AM
Dallin Law PSP

Thanks, L, this is useful information I have sought this matter with internal counsel however they seem reluctant or unable to find the case law. When facial recognition is brought up trepidation is inherent so I just want to gather information see what the potential is for the fallout. This is an excellent resource thanks for your help.

Dallin Law, PSP
Physical Security Professional
Utah State University
Logan, Utah
USA

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 12 May, 2021 04:13
From: L. Lanark Lockard
Subject: Video Surveillance Case Law

Dallin,
I am NOT an attorney; however, I found a case in the 9th US Circuit Court of Appeals that indicates there are some expectations of privacy regarding being tracked through facial recognition by private organizations (non-law enforcement), in this case it was Facebook. A Federal Court Sounds the Alarm on the Privacy Harms of Face Recognition Technology | American Civil Liberties Union (aclu.org).

I would recommend you contact your general counsel at Utah State University. This is an unsettled area of law and may differ in other US Circuit Courts and State Appellate or Supreme Courts.

L. Lanark Lockard
Specail Agent (retired)
Retired from Naval Criminal Investivative Service
Kailua HI
United States

top previous next

9. Re: Video Surveillance Case Law

Reply to Group via Email | Reply to Sender Online



May 12, 2021 11:48 AM
Jon Polly PSP

Dallin,

I don't have the case law, and I am NOT a legal expert, however I may have some insight based on experience.

I remember a training back in the analog camera days that a case in Florida Federal Court required all cameras to record at a minimum of 7.5 Frames Per Second (fps) to 12 fps to be admissible in court. I have always used that as a standard when deploying camera systems. Also, recently I have understood that courts have let the gaming industry run at 15fps vs 30fps because the difference is so minute to the visible eye, along with storage savings the need for 30fps was not there.

In regards to facial recognition, there are a number of court cases pending on this. Something to note on facial recognition is that the term is a broad statement for multiple technologies. There are three distinct buckets here and only one is really being challenged. Depending on what technologies are being used, the old saying of "reality is not reality, but perception is reality" comes true. Facial recognition must be articulated well, and there is no guarantee that perception won't drive reality.

1) Face Matching technology - named multiple things - This is software that takes a known picture and scans recorded video for a likeness. Anything over a 75 percent hit is flagged as a possible match. This requires human interaction to review and accept or throw away. It is a great technology for investigations, tracking where a person was last seen, or for tracking in a stadium / retail applications for buying trends.

2) Facial Recognition technology - This is the one being challenged - Accuracy of between 85% and 93% on good systems (not datasheets, these are skewed). This requires a known picture or a learned picture to be "recognized" in real-time and then an automated workflow to do "x". "x" could be alert security, initiate lockdown, etc.

3) Identity and Access Management (IAM) biometric - this one is still just coming out - IAM is the same concept as facial recognition to unlock a cell phone. IAM facial recognition biometric is used by an access control system to unlock doors via facial biometric. The accuracy of this product must be higher than 99.5% and must be limited to within 3' of the door being unlocked. Unlike the other two technologies, the participant is willing and has been learned into the system.

As for ALPR technology, again I don't have the cases to cite, however when dealing with citywide applications, the license plate is considered public. It is procured through a state agency and there is no right to privacy as it is mounted on the exterior of the vehicle. Some police departments have internal SOPs about how they can run a plate; however, on a campus application, the person driving has entered a place of higher learning with no expectation of privacy to the tag. ALPR can be used on campuses for criminal action / investigation, as well as for revenue generation through parking. Many of these use the same system and are separated via users to what data they get access to. If the campus has a recognized police department, they can have access to the FBI's National Crime Information Center (NCIC) database, depending on the system being used.

For ALPR there is also two things to remember, there is License Plate Capture - A cctv camera running an analytic - 85% accuracy, and then there is an ALPR / ANPR camera that is specifically designed for license plate recognition - 97%+ accuracy on license tags only.

LPC and ALPR data can be used in most courts without issue.

Can you be held culpable? Only if the technology is installed and turned off. This plays to a crime or injury, but just like a dummy camera, if it is installed and a crime happens underneath it, then the campus may be open to civil case by the injured party. This can also hold true if a camera is down for maintenance and has not been fixed. As long as the service request can be tracked that the camera was down, a replacement was ordered, etc, then the campus may not be at fault; but this would need to be addressed with legal counsel.

@Donald Zoufal CPP

My signature is below, feel free to reach out if I can be of further assistance.

Jon

Jon Polly, PSP, IC3PM
Chief Solutions Officer
Protecht Solutions Partners, LLC
Charleston SC
United States
www.protechtsolutionspartners.com

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 11 May, 2021 17:39
From: Dallin Law
Subject: Video Surveillance Case Law

Does anyone have a resource or a list of Case Law or Jurisprudence in regards to video surveillance systems use? Most particularly in places of higher education.

We are having issues with identifying the unknowns in the way of should we have facial recognition. What does that do to the image of the Higher education institution?

Should we record license plates can these be used in a court of law. If so what legal requirements must be met in order to have strong evidence for the purpose of the trial? Can we be held culpable if we have certain capabilities but not utilize them?

I'm looking for case law or lessons learned in this area so we can apply policies and procedures and deploy technology appropriately to protect ourselves and students/guests.

Dallin Law, PSP
Physical Security Professional
Utah State University
Logan, Utah
USA
---

10. Re: CPP Study Groups for Exam Review

Reply to Group via Email | Reply to Sender Online



May 12, 2021 12:26 PM
Roy Parks CPP, PSP

Hi Mike / Hi Suzanne,

Robert Natoli from the Sacramento, CA ASIS Chapter is hosting a CPP study group right now. I did his PSP study group and it was excellent! I'm on the East Coast and the study sessions started at 5pm Pacific Time and lasted 1.5 - 2hours.

I reached out to him and he will said; "If any of your people are interested in joining the one I'm in the middle of, I would be happy to give them a 50% off discount so it's only $100. They would have full access to the entire PowerPoint library and all of the recordings of the first four sessions they missed."

Each session is recorded and available for download after they're conducted. I was able to review all of the material before I took my exam, which really helped.

If you (or anyone reading this post) want to participate, contact Robert at Robert@NatoliConsulting.com and he will send you a link and a discount promo code. Let him know I referred you to him.

Mike - I lived in Roseville before I moved to Virginia. I enjoyed living there. A well run city and nice that it has it's own power plant.

Let me know how you do!

Best!

Roy Parks
rparks@kroll.com

Roy Parks CPP, PSP

Senior Manager
Kroll, a division of Duff & Phelps
Broadlands VA
United States

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 11 May, 2021 23:52
From: Michael Clayton
Subject: CPP Study Groups for Exam Review

Hi All,

I'm also looking for a CPP study group.?? I'm in Roseville, CA, and I'm a member of the San Francisco chapter.?? Regards,?? Mike Clayton

Original Message:
Sent: 5/10/2021 8:53:00 AM
From: Suzanne Altimore
Subject: CPP Study Groups for Exam Review

Seeking an upcoming study group or exam review for the CPP. Prefer Eastern time zone.

Thank you in advance.
Suzanne Altimore

Suzanne Altimore
Global Security Programs & Compliance Manager
G4S
HARDEEVILLE SC
United States
---

top previous

11. Re: Passed the CPP Certification Exam

Reply to Group via Email | Reply to Sender Online

May 12, 2021 2:27 AM
Dinesh Mohanaraj

Awesome. Congratulations

Dinesh Mohanaraj
Operations Executive
Security & Risk Solutions Pte Ltd
Singapore
Singapore

Reply to Group Online **View Thread** **Like** **Forward**

Flag as Inappropriate

Original Message:
Sent: 10 May, 2021 03:56
From: Joseph Gwei
Subject: Passed the CPP Certification Exam

Grateful to announce, that I passed the CPP certification exam in my first attempt.

Joseph Gwei PSP
Security Manager
GROUPE ALUCAM
Edea
Cameroon

You are subscribed to "Open Forum" as paul.upton@pol.state.ma.us. To change your subscriptions, go to My Subscriptions. To unsubscribe from this community discussion, go to Unsubscribe.

From: Axon
To: McCarthy, Steven (POL)
Subject: Our in-car webinar is this week - register now!
Date: Tuesday, October 26, 2021 3:42:01 PM

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

Axon

Hello Steven McCarthy,

In case you missed it, we have an exciting webinar coming up this week.

Dallas Police Department will walk you through their decision to use Cradlepoint's 1700 router and their experience testing Axon Fleet 3 in-car units.

Axon and Cradlepoint's partnership has made strong connectivity the standard in in-car video, now and in the future, as 5G continues to evolve what's possible. Come discuss the future of wireless connectivity with us as we connect officers to the command center, surveillance cameras, ALPR, drones, and more.

Thursday, 10/28 at 12 pm PT/3 pm ET

REGISTER NOW

Sincerely,
The Axon Team and our partners at Cradlepoint

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The Delta Logo, Axon, and Axon Citizen are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information visit www.axon.com/legal.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

Contact Us





From: Police1 Roll Call
To: zzJoyce, Gina (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:15:03 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

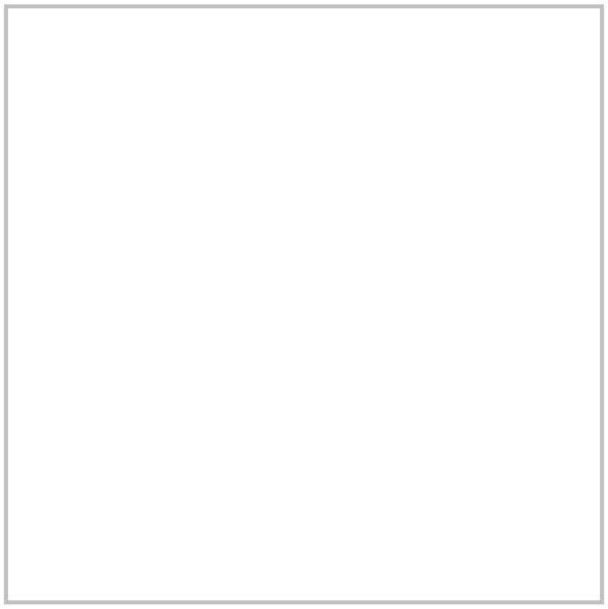
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

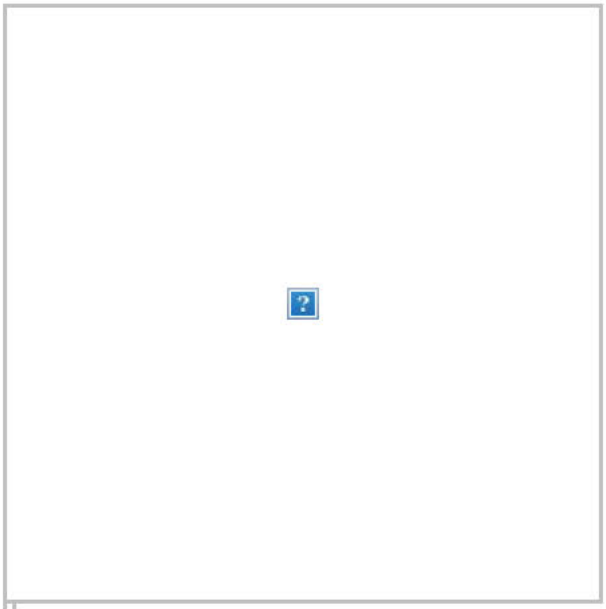
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzLee, Brian (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:14:54 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

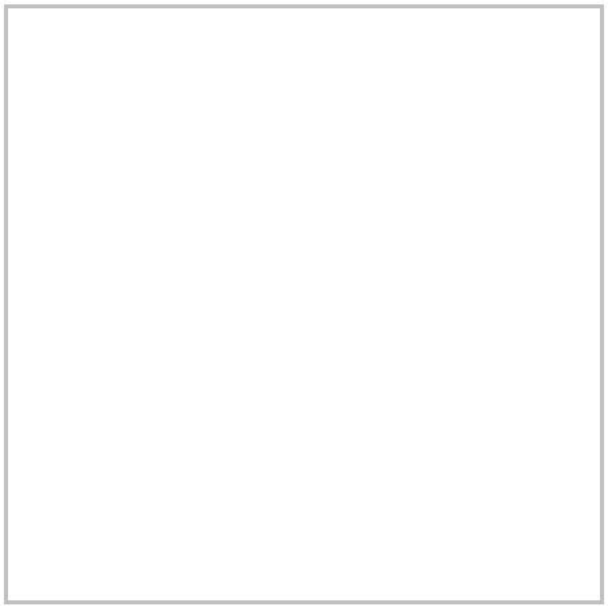
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

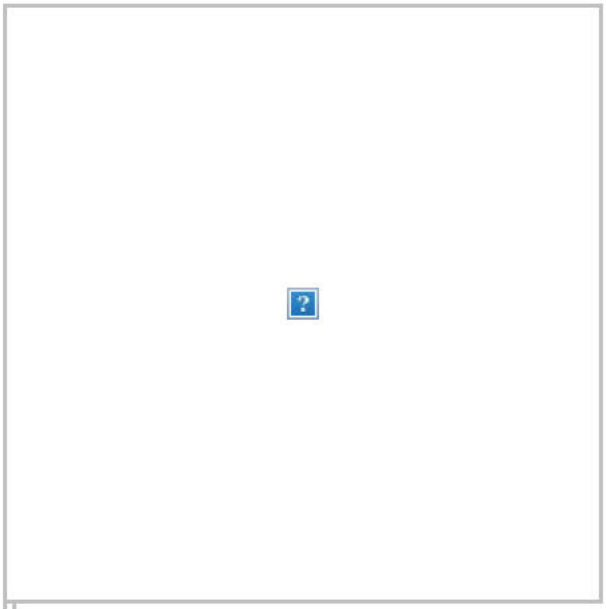
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Paquette, Brian (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:13:36 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

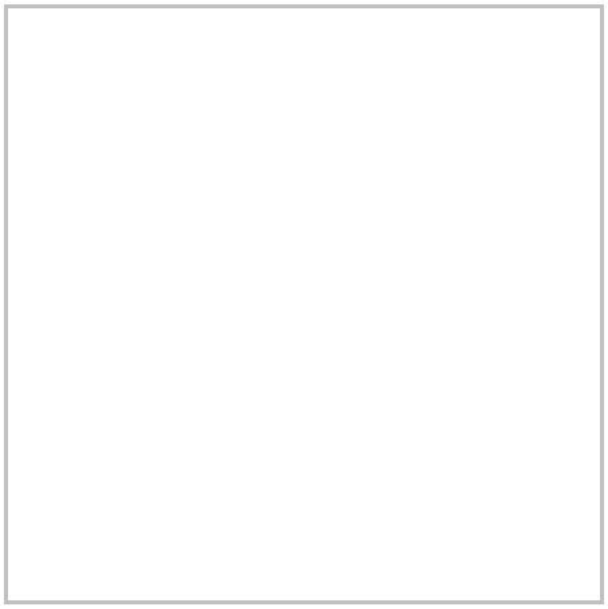
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

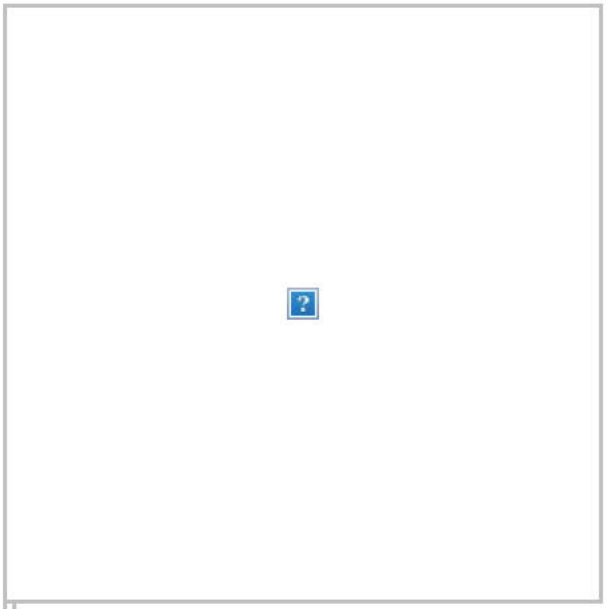
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Mcginn, Daniel (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:13:31 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

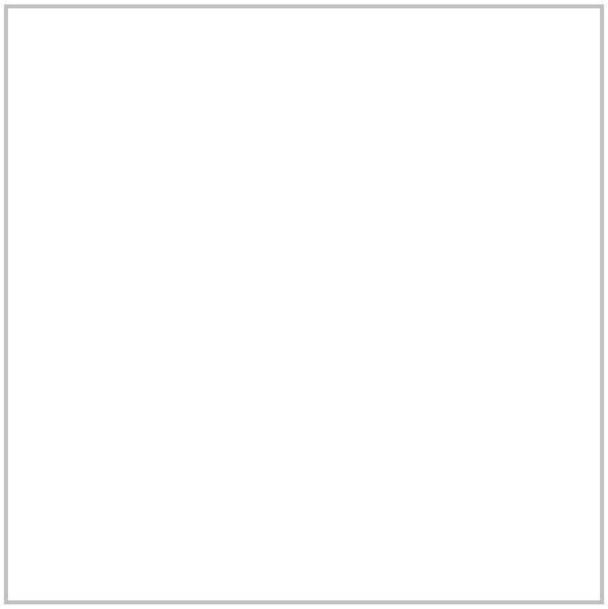
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

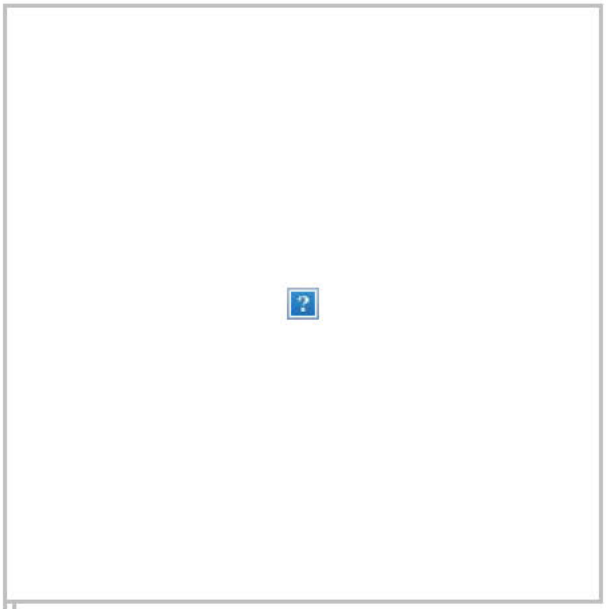
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Upton, Paul (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:13:24 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

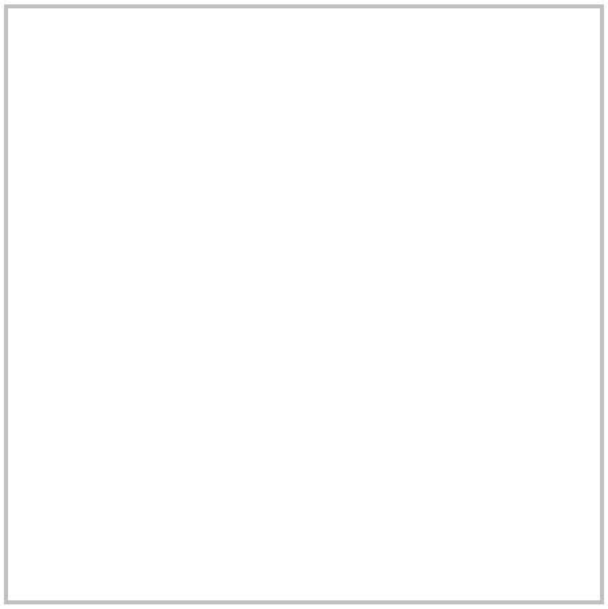
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

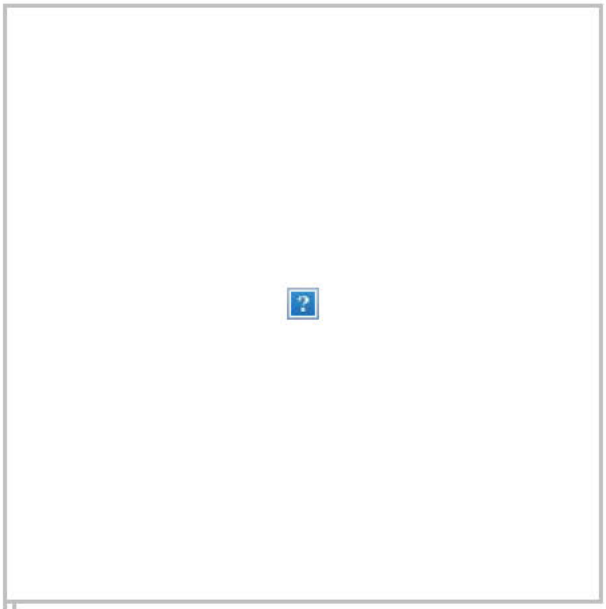
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lavoie, Marc (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:13:08 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

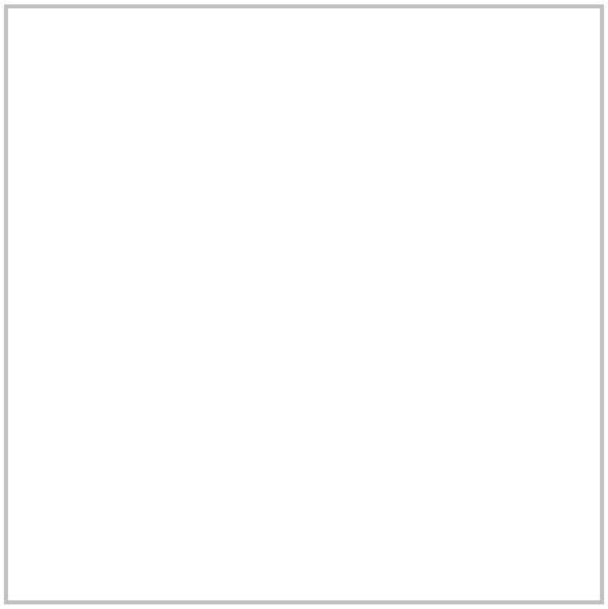
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

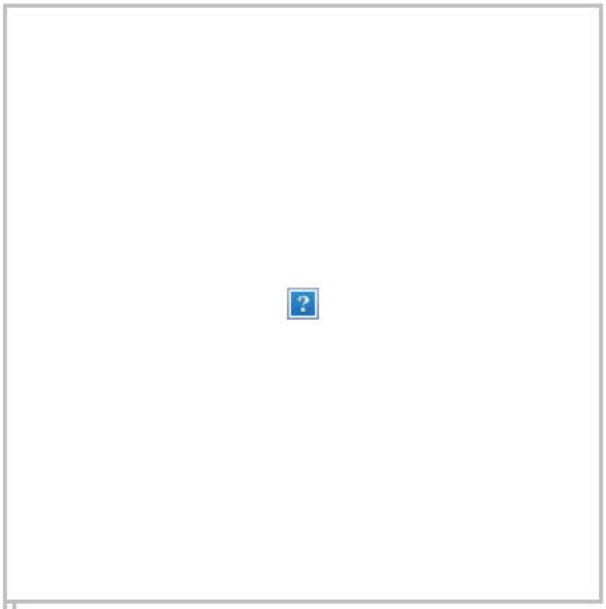
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



FEATURED CONTENT

Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cooper, Brian (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:13:04 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

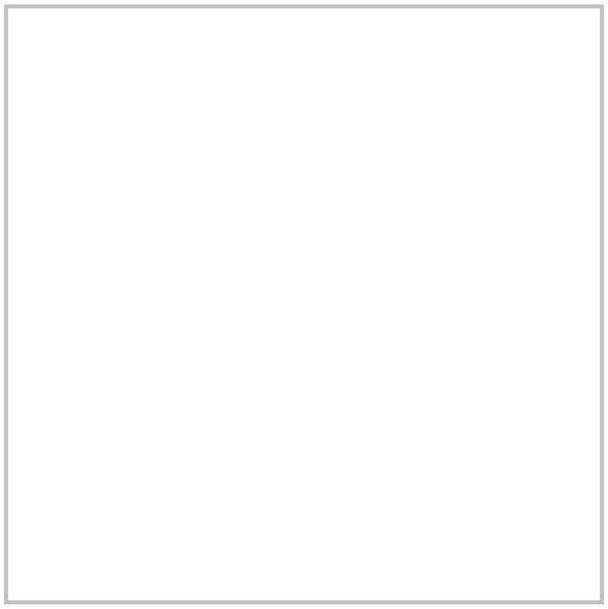
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

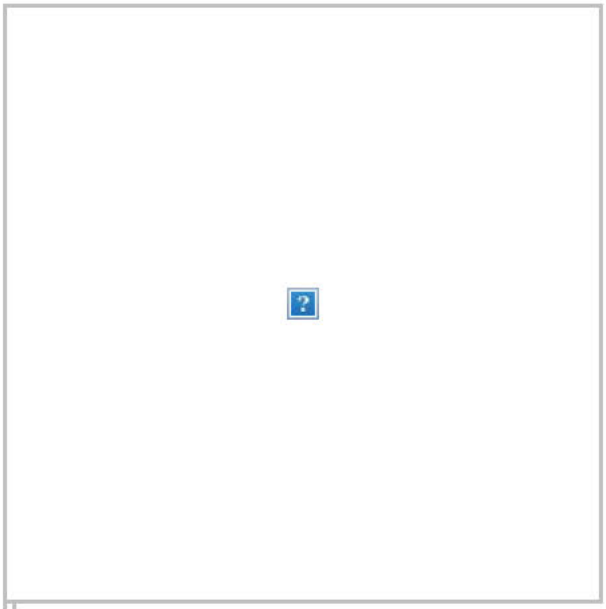
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work



In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety



ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Irwin, Patrick (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:13:02 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

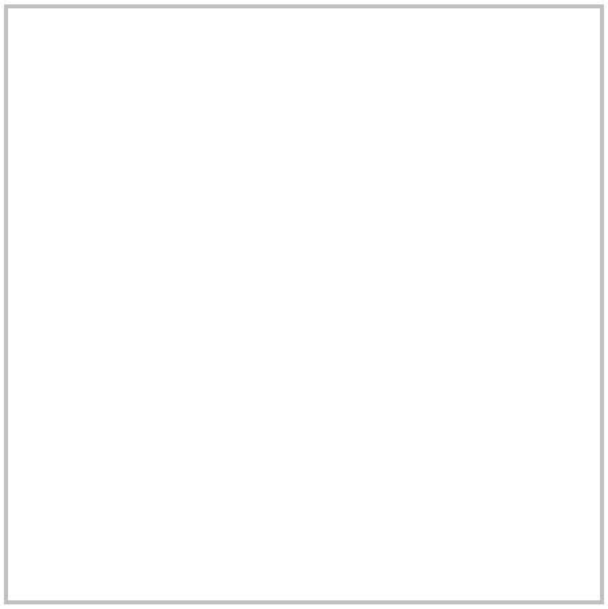
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

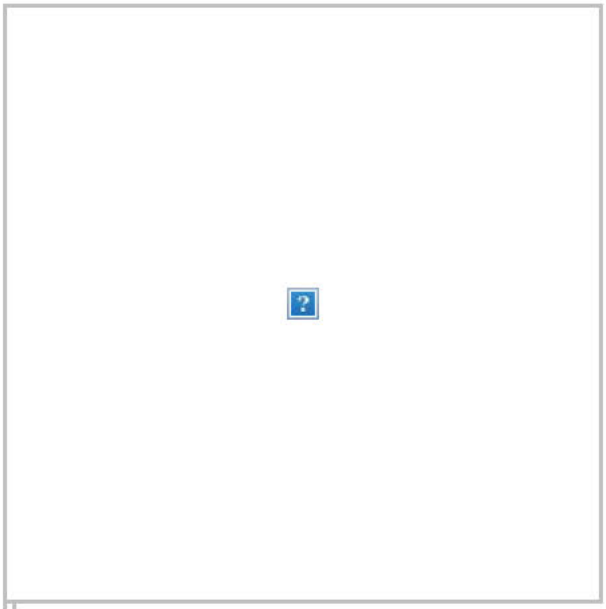
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cronin, John E (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:12:57 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

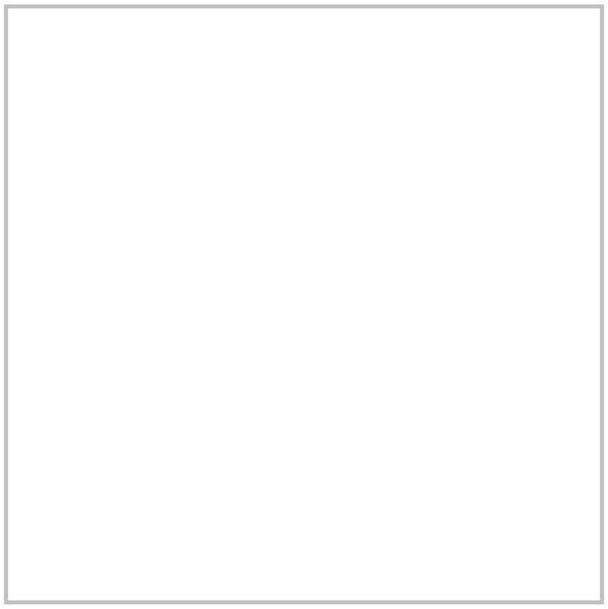
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

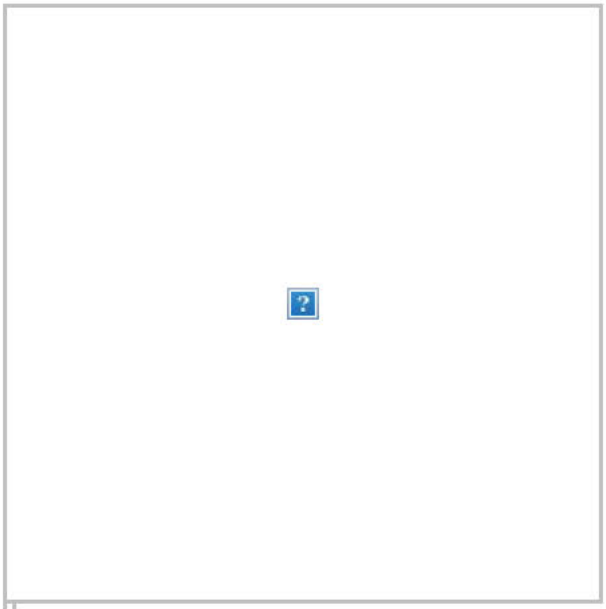
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cronin, John E (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:12:13 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

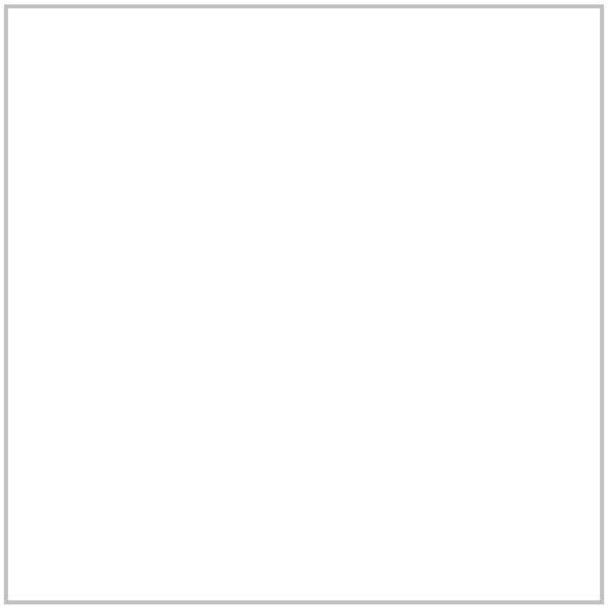
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

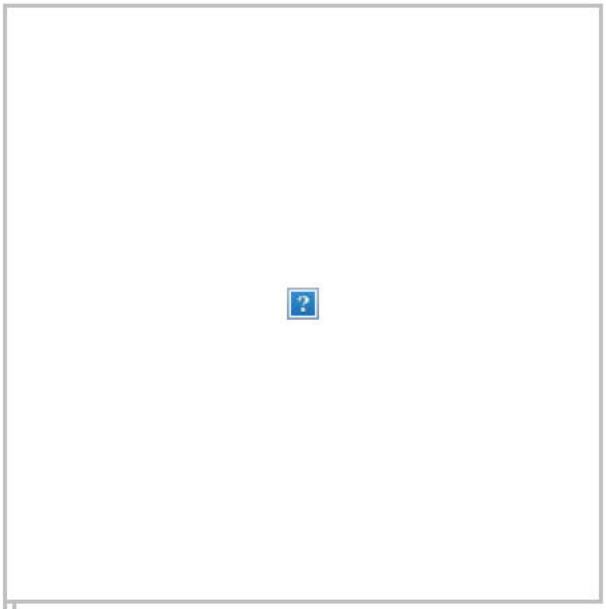
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Rizos, Byron (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 3:16:33 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

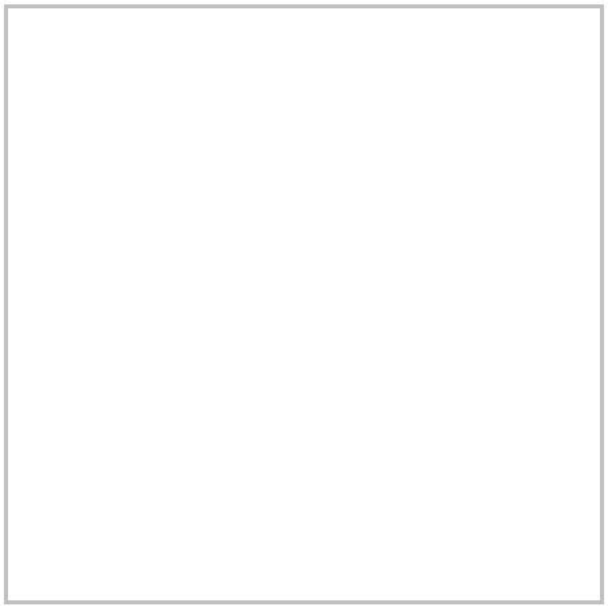
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

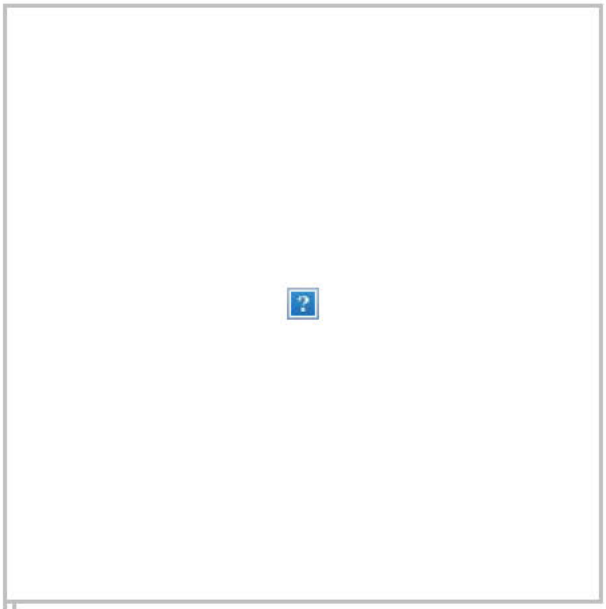
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzNee, William (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 3:14:57 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

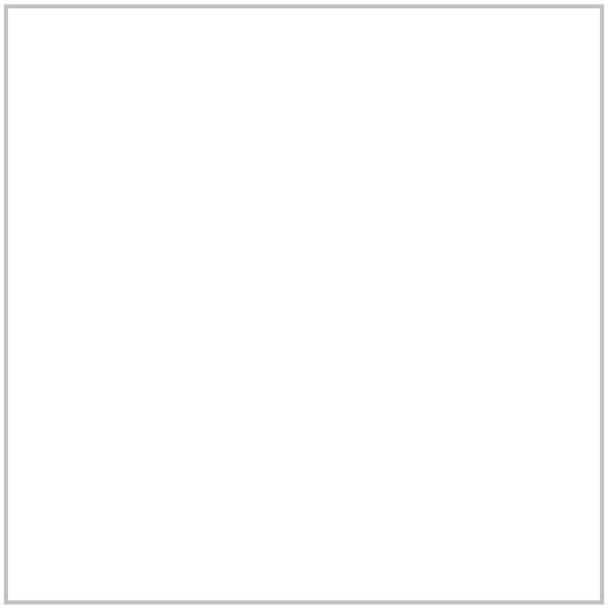
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

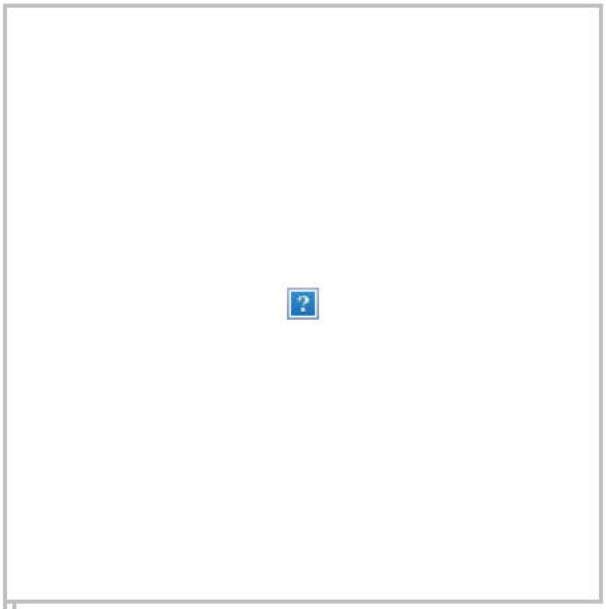
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lawlor Jr, Daniel (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 3:13:22 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

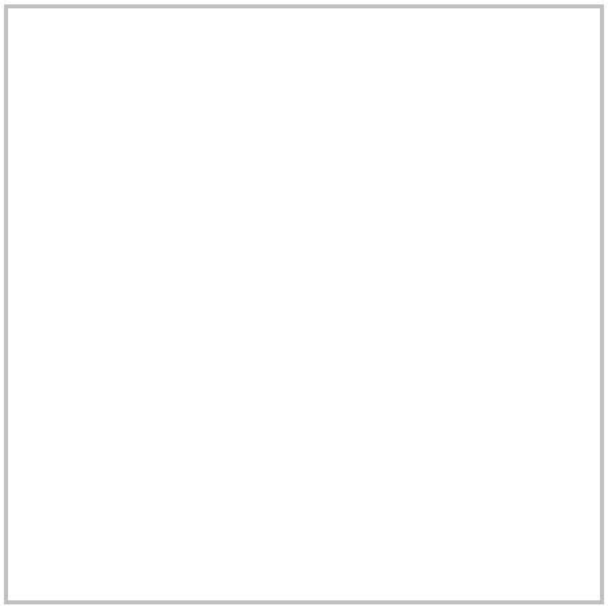
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

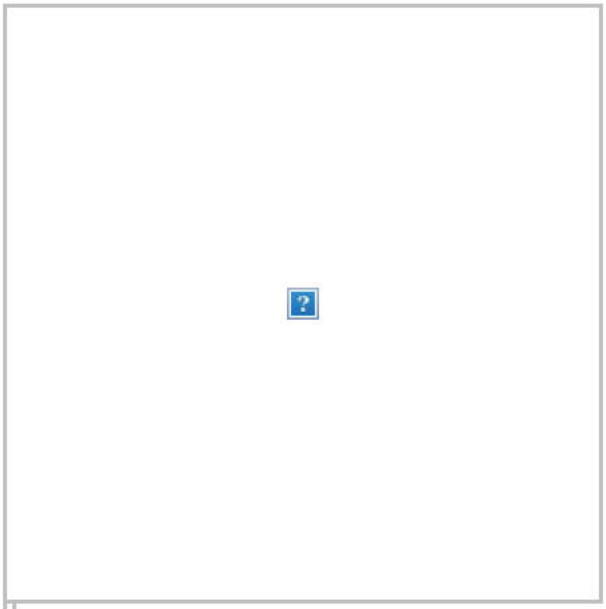
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work



In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety



ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzJohnson, Robert - Captain (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 3:13:00 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

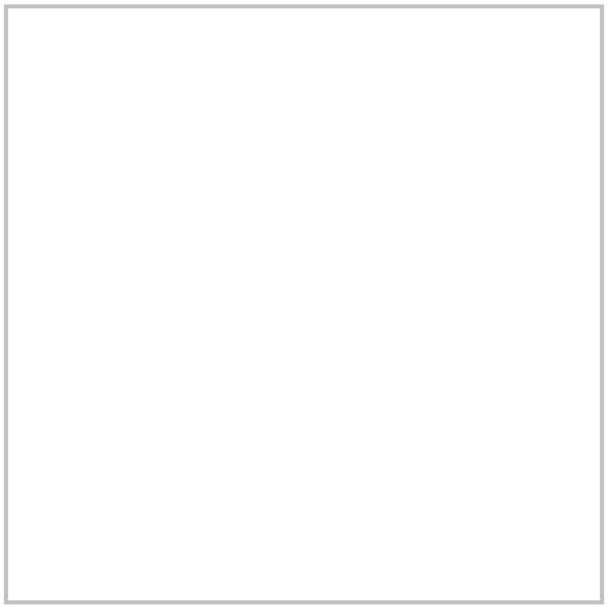
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

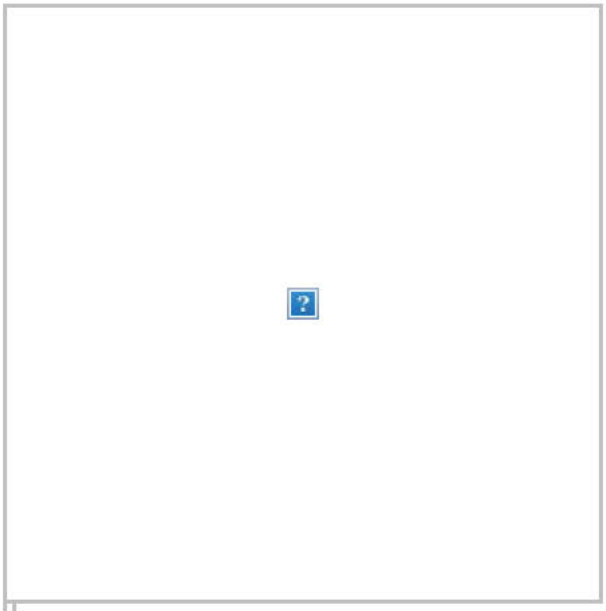
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



FEATURED CONTENT

Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 3:12:51 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

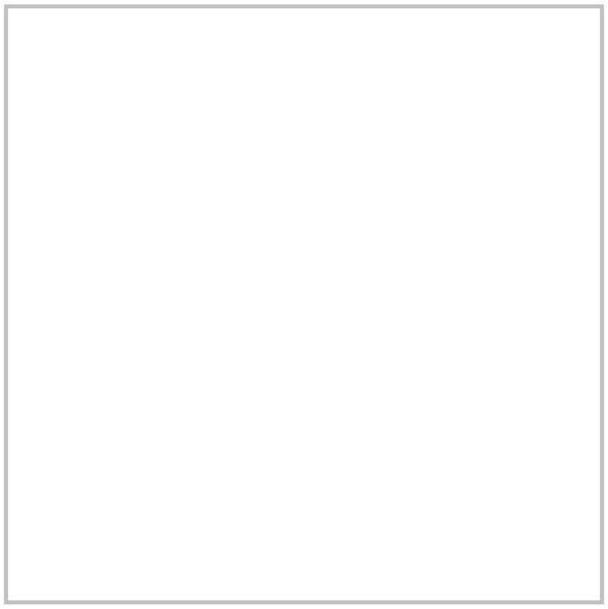
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

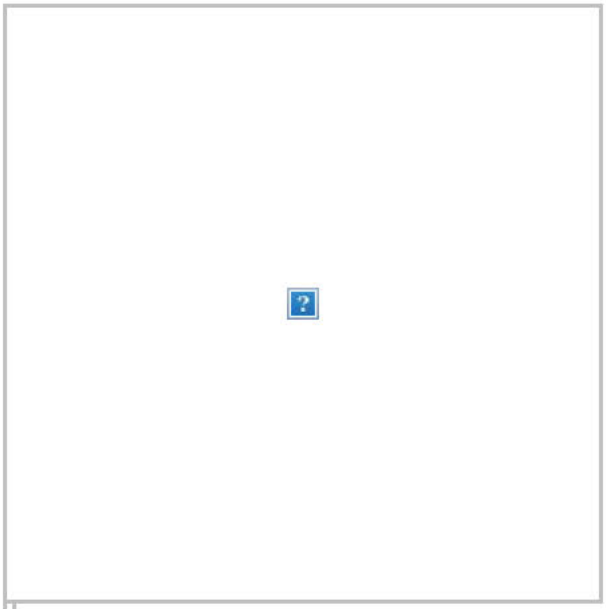
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Clement, Michael (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 3:12:42 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

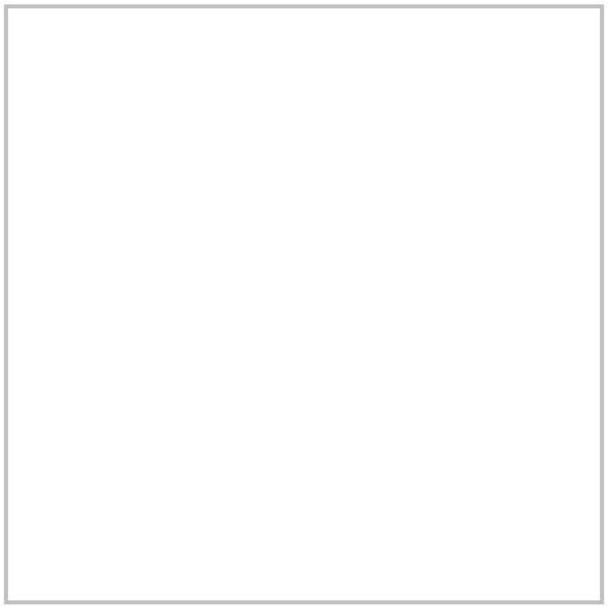
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

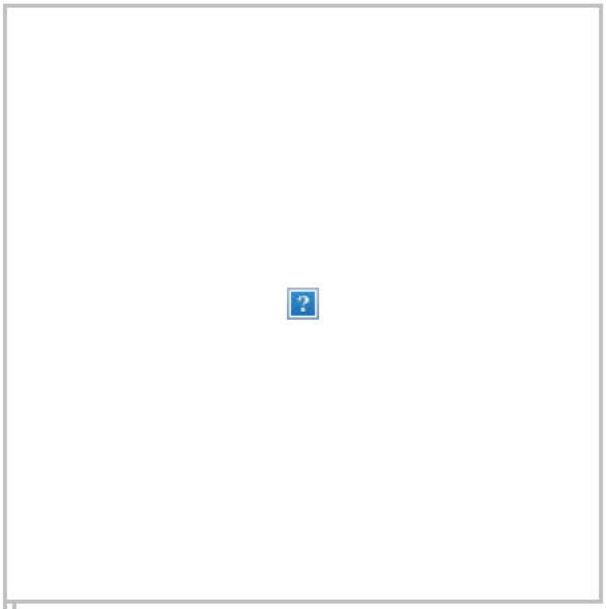
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Golenski, Michael (POL)
Subject: Philly bans minor traffic stops; Chicago PD"s vax mandate battle
Date: Friday, October 15, 2021 6:17:16 PM

October 15, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Tomorrow is National Move Over Day, the annual reminder for drivers to slow down and move over when approaching stopped emergency vehicles and responders, tow trucks, and utility or maintenance vehicles when warning lights are flashing.

More than 150 law enforcement officers have been killed since 1997 after being struck by vehicles along America's highways. We urge you to not only educate your community about how Move Over laws keep cops safe, but also educate yourself about highway safety best practices.

Here are some tools to add to your safety toolkit:

► A Gordon Graham webinar on keeping cops safe during highway ops

► A guide to setting up a safe work zone at a roadway incident

► An LEO motor struck-by infographic to identify risk factors.

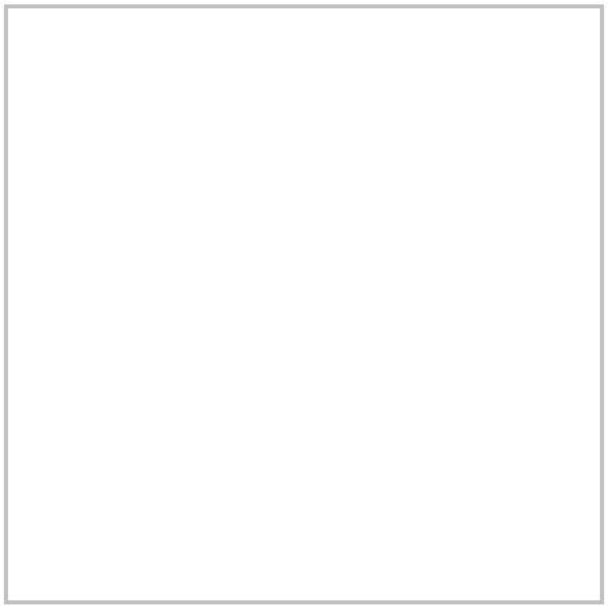
Stay safe,

— *The Police1 Team*

TOP STORIES

Vaccine mandate stalemate: Chicago mayor seeks legal action against FOP

Union leader John Catanzara has told members to defy the mandate. Mayor Lori Lightfoot warned of discipline if they do



Wounded Chicago officer, partner of slain Ella French, is released from rehab

Handcuffed Fla. man steals police car, leads pursuit for 70 miles

Hackers deface 4 Okla. sheriff's office websites

Philly bans traffic stops for minor infractions

'Real consequences': Fla. sheriff warns students against TikTok challenges

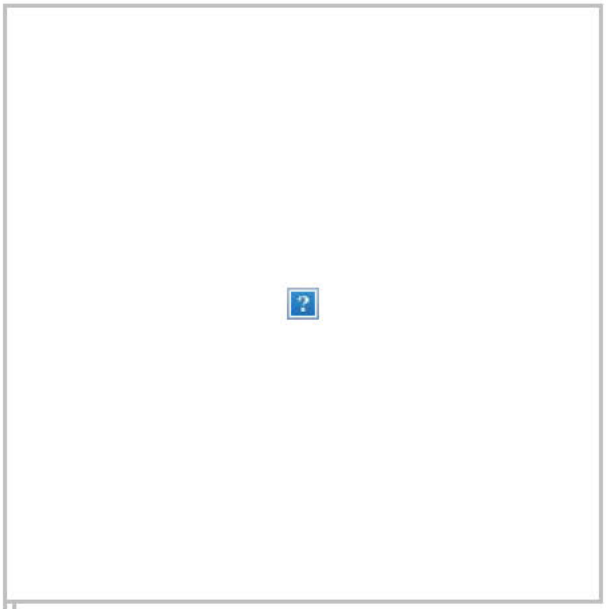
Baltimore Police union tells officers not to reveal vaccine status as deadline nears

Go From Total Station to Total Solution!



Learn how the Clackamas County Sheriff's Office benefited from a FARO Focus Laser Scanner and has cut time spent on scene in half and saved thousands in overtime costs.

Learn how



Building leadership capital with your cops and your community

By Policing Matters Podcast

Chief Roger Schei of the Pocatello Police Department discusses the mindset required to be an effective law enforcement leader

Why we must move 'Move Over' up the agenda

By Rob Lawrence

As law enforcement officers continue to be killed on our nation's roadways, we must continue to message about the importance of "Move Over" laws

Photo of the Week: On campus

By Police1 Members

College students get to know law enforcement recruiters at a career fair in Maine

Meet the Printers That Work Where You Work

In today's data-driven world, relying on outdated paper-based systems is practically a crime. Save your department time with rugged, compact PocketJet® and RuggedJet® printers from Brother.

Explore the Printer Mount Solutions

How 'Green Cameras' Can Improve More Than Just Traffic Safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous greenhouse gases.

Learn more

NATIONAL POLICE WEEK

33rd Candlelight Vigil honored 701 fallen LEOs during Police Weekend 2021

By Police1 Staff

Each officer's name was read as a part of the ceremony and etched on the walls of the National Law Enforcement Officers Memorial

Police Week poem: Between the Monsters and the Weak

By Michael Marks

This poet pens a moving tribute to the men and women of law enforcement

250 miles on the road to recovery

By Cole Zercoe

Officer Ashley Wilson's partner was fatally shot in the line of duty. Her journey to heal took her on a three-day bike ride to honor his memory

SPONSORED CONTENT

Increase performance and build trust using tactical intelligence (white paper)

Find out how powerful software programs can provide actionable intelligence that helps law enforcement agencies solve, reduce and even prevent crime.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 198 grain Dual Performance round

FEATURED DEAL



Get Protection and Comfort from Body Armor Built by Military Experts

Learn more

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Nancy Perry, Police1
To: McCarthy, Steven (POL)
Subject: Policy review boards | Relationship-based policing | ALPRs in action
Date: Wednesday, July 21, 2021 4:46:44 PM

July 21, 2021 | View as webpage | Too many emails? Update Subscription Preferences

Leaders,

At the end of last year, we asked police leaders and law enforcement subject matter experts to outline solutions for the issues facing the profession in 2021. Topics addressed included community relations, counterterrorism, officer wellness and police reform. At this halfway point in the year, let's see how accurate our experts' predictions are to date. Check them out here. It's not too soon to think about both the challenges and opportunities facing law enforcement in 2022. Email your predictions to editor@police1.com.

P.S. We need one minute of your time. Police1 is evaluating current online training needs for law enforcement and would like to get feedback from police leaders on what you think can make a difference in your department. Click here to complete our short survey.

Stay safe,

— Nancy Perry
Editor-in-Chief, Police1

FEATURED CONTENT

Motivational conversation for community building

By Al Cobos



Community building is a foundational aspect of good policing. In today's modern society where traditional media, activist groups and proactive individuals supply a constant stream of information on social media, law enforcement must establish a core relationship with the multifaceted communities where we provide services. Motivational conversation is a process that can help your agency improve its relationship-based policing.

At its core, motivational conversation is about creating conversations that lead people, groups, communities and organizations in the desired direction of positive change. As with any relationship, it takes honesty, commitment and effort to achieve meaningful connections.

Ask versus tell

Motivational conversation begins with the use of questions to create dialog that will move a person, group, or entity in a specific direction. This is the "ask versus tell" approach to conversations. It is very easy for police to "tell" people what they need to do to achieve positive change. The challenge is to "ask" a question when we feel the need to "tell" someone what to do.

The asking is not from a position of potential weakness (will you do this task for me?) but from a position of inquiry that leads to the goal (how can this task be accomplished?). We must use the same approach when building community relationships. Too often we “tell” communities what needs to be done instead of “asking” what needs to be done to achieve a common goal. Asking leads to genuine dialogue, which over time will move a community and a police agency in the right direction.

Creating questions

Questions should be open-ended where they cannot be answered with only a one- or two-word response. Use the following process when creating questions for community engagement:

- **Intent**: Does the question lead the community in a specific direction?
- **Conversation**: Do the questions create valuable conversations with a community?
- **Relationships**: Do the conversations with the communities build genuine working relationships?
- **Results**: How can I measure/quantify that we are heading in the right direction for everyone involved?

The Intent-Conversation-Relationships-Results process for creating questions will create the engagement and goal-oriented solutions that we strive for in our community-building efforts. This process is also good to use when speaking to line personnel, administrative staff, executive teams and organizations. Once you have incorporated this process into how you create questions, it will become second nature and it will improve your ability to influence others.

Community building questions and goal setting

Leading people can be positional (rank) or relational. Motivational conversation occurs in a relationship-based interaction between law enforcement and communities. The following provides a template for the types of questions to ask to create the groundwork for community building that will involve goal setting as part of the intended process. Modify the questions to suit your agency’s specific needs.

What is our reason for engagement?

- What is the reason for attempting this process?
- What are the benefits of engagement?
- What are the consequences of not taking action?
- If we do not attempt engagement, what group or entity will? Will that other group create engagement or conflict?

What skills can be brought to the table by each side?

- Are there people in the groups that have commonalities?
- Who are the collaborators in each group?
- What individuals can be counted on to promote a common goal, especially when there is conflict among the groups?

What perspectives does each side bring to the conversation?

- What is the most significant perspective that must be contended with to create a conversation for change?
- How will the predominant perspective affect engagement between groups?

What is my role?

- What are my responsibilities as an individual, a representative of my profession and a representative of affiliated groups?

Who can be counted on for help or guidance?

- Can help be found within my group or can it be found with the community that is being engaged?
- Is there a third party that can be contacted to help?
- What can I learn so I can be a resource for others in this process?

How will conflict be resolved?

- Will there be a set of informal/formal rules to address conflict?
- How will conflict be handled which is created by your group?
- What is the expectation of handling conflict for the group you are connecting with?

These questions are intended for both law enforcement and the community that is being engaged. Use them as a starting point to have a better outcome during the community-building process. It is recommended that this questioning process be provided to the leaders of the involved group. It could be a key icebreaker for dialog while laying out the expectations for each side by utilizing the intentional questioning process.

***NEXT:** 4 ways officers can improve neighborhood relationships*

Can AI-powered drones improve policing?

Learn how crime and crash scene investigations could be improved with drones integrated with connected vehicles and devices with Carl Blando, sergeant detective, Boston Police Crime Scene Response Unit, and Police1 live on July 28.

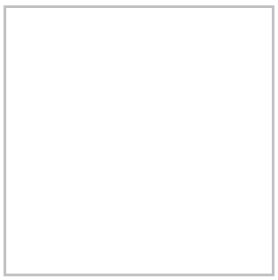
Register now

10 tips on conducting a community review board for police policy

By Lexipol Content Development Team

Increasingly, law enforcement agencies across the country are organizing and implementing community review of their policy manuals. These departments, communities and community review board members should be commended for their commitment to safe, effective and community-specific policing.

But conducting a community review board for police policy requires clear



expectations, well-defined roles and terms, and identified policies that are up for review. It's critical for agencies and committee members to enter the review board process with a set process and common goal in mind to avoid disillusionment and ensure meetings and recommendations are productive.

We've compiled the top 10 recommendations from law enforcement experts when it comes to developing and working with a community review board on police policies. Departments should have at least one representative from the agency, alongside a diverse set of committee members that represent the different languages, ethnicities, perspectives and professions of the community.

With such a diverse group, it's exceedingly important to ensure everyone is on the same page and unified in the goal of creating safe, effective and relevant policies.

1. Provide opportunities to speak: Leaders must guard against the potential for some members of the review board to dominate the discussion. Because the purpose of a community review board is to have the agency and community benefit from a diversity of perspectives, make sure a single point of view does not dominate, allowing all participants to have the chance to have their voices heard.

2. Educate committee members: Most committee members likely have knowledge of law enforcement operations and policy limited to what they have seen in movies and TV. The agency should conduct training and/or orientation for review board members to offer them greater insight and shared knowledge of policing practices.

3. Define terms: Commonly used policy language must be defined to create a common understanding among all community review board members. When terms such as “shall,” “should” and “may” are properly defined, committee members can more accurately understand and weigh in on potential policy changes, knowing the role of specific legal language.

4. Set roles and boundaries: Make sure committee members are aware of what their role is on the review board and in policy recommendations and updates. Determine how differences in opinion on the board will be reconciled and clearly explain how suggested policy changes will be accepted or rejected by department leadership and why. This will help avoid frustration and disillusionment within the committee and from the public, increasing transparency and accountability.

5. Choose policies: It likely isn’t feasible to review every single policy in your policy manual – and your committee probably isn’t interested in your sick leave, travel or email policies. As your department establishes the community review board, take time to decide which policies from your manual the board is slated to review. Common policies include use of force, handcuffing and restraints, and hate crimes.

6. Maintain community focus: While it can be easy to focus on national or regional incidents involving police, community review boards must stay focused on their own community. In doing so, committee members can limit distractions and ensure community issues are front and center in every meeting and discussion.

7. Understand transparency and collaboration: Agencies should strive to be fully transparent

about every policy, but it's important to be clear about what policies are up for debate and which are not. Community review boards provide a unique opportunity for police-community engagement and collaboration, but police and community safety must remain the central focus – and sometimes, specific policies and policy language are the way to accomplish that.

8. Remember federal and state laws: Policy content based in federal or state law should remain relatively unchanged. Remember, while your committee and community may desire a policy language change, that doesn't change the language or letter of the law. Limit these types of changes to ensure your agency and community are in line with what the law calls for.

9. Avoid semantics: Don't allow the community review board to get caught up in semantics. Does the word change impact the legal meaning of the policy or the way the policy affects operations? If so, in what ways? If not, the change is probably unnecessary. Limiting changes based on semantics can help save time and effort for all parties.

10. Align policy and practice: When policy and practice don't align, the disconnect can be devastating and discouraging to committee members and the community as a whole. As you review policies and recommendations, see how they currently align with your practices and how practice may need to change as a result. Is each policy applicable, practical and functional? Are the policies possible and reasonable to implement? Preparing for this reality ahead of time and appropriately setting your, your personnel and the community review board's expectations can make all the difference.

When done right, community review boards can be incredibly effective, giving community members a voice and improving the safety and professionalism of the police force. Not only do these committees help build trust between the community and law enforcement, they also lead to community-centric policies that address the specific needs and priorities of those you serve.

***NEXT:** Community review of law enforcement policy (white paper)*

TOP TWEET: ALPR TECHNOLOGY

BE ADVISED

3. ALPRs in action: San Mateo County Sheriff's Deputy David Brandt discusses how ALPRs identify stolen cars, help locate missing people and track traffic conditions to determine if changes need to be made to increase safety.

2. How Oklahoma reduces risky traffic stops: The UVED Program uses low-cost vehicle and license plate recognition technology to proactively identify uninsured drivers.

1. How to buy license plate readers: Whether you are leading a purchase for the first time or looking to upgrade your department's equipment, this Police1 guide is a starting point for your purchasing process.

Police1 does not send unsolicited messages. You are receiving

this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Portland PD unit"s mass resignation memo cites "extreme liability"
Date: Monday, June 21, 2021 4:12:27 PM

June 21, 2021 | View as webpage

Dear Police1 Member,

If you believe data breaches, cyberattacks and ransomware are not areas of risk for law enforcement, think again. Here are some recent headlines that show public safety is as vulnerable to cybercrime as the private sector:

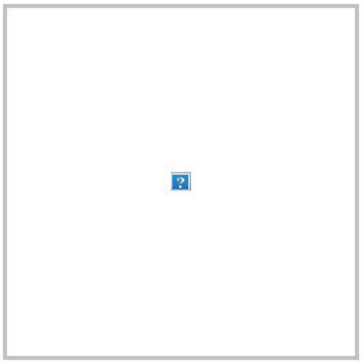
- 'BlueLeaks' exposes files from hundreds of US police departments
- DC police department hit by apparent extortion attack
- NYC's law department targeted by cyberattack

Join a panel of experts on June 24 for an interactive discussion, sponsored by Tyler Technologies, on cyberattack risks and preparation. Panelists will discuss recent cyberattacks and threats on public safety agencies and detail how your agency can develop a defensive strategy for these unprecedented attacks. Register here.

Stay safe,

— The Police1 Team

TOP STORIES



Portland crowd control unit leader: Officers can't serve under 'the extreme liability'

Portland's Rapid Response Team made headlines last week when, in an unprecedented move, its members all voted to resign

A N.M. cop lost his leg in a motorcycle crash. Now he's a motor officer

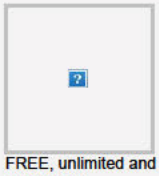
Minn. PDs hand out vouchers to repair broken car lights instead of tickets

LAPD offers community programs over jail time for certain crimes

Police: Woman shoots at officer during Juneteenth parade, is killed

Iowa deputy shot multiple times triggers manhunt

Get Free Grant Help for CentralSquare Public Admin Solutions



To help you find applicable grants and secure additional funding for your budgets, we've partnered with GovGrantsHelp to offer FREE, unlimited and customized grant assistance.

Learn more

Rekor Finder: Powerful & Discrete in-vehicle ALPR



Finder is a cost effective in-vehicle ALPR solution that accurately identifies license plates and vehicles in real-time, at high speeds and extreme angles.

Learn More

FEATURED CONTENT



Incorporating the 'tenth man' concept into critical decision-making

By James Dudley

An independent examination of intelligence should be considered in planning for an event or responding to a real-time, unplanned incident

A weekend of firearms instruction by John Hearne cannot be missed

By Warren Wilson

Hearne has done an amazing amount of research into the brain and how it works under stress

1-click Prime Day tips for public safety

By Greg Friese, MS, NRP

What's on your department's Amazon wish list? 5 ways to leverage Prime Day for your department and community

HIRE SMARTER with Background Investigation Software

Stand out from other agencies and demonstrate your commitment to hiring quality law enforcement professionals while minimizing your community's risk.

Watch a demo now

banner1 jpg?w=300&format=jpg&quality=87

LEADERSHIP ISSUES

Why law enforcement executives should maintain their physical fitness

By Deputy Chief Benjamin M. Murphy

Whether you choose weightlifting, CrossFit, running or cycling, it benefits an agency to have a healthy, strong chief

How police leaders can provide psychological support after an OIS

By David Black, Ph.D.

Law enforcement officers involved in a recent shooting require support from the top to process potential trauma

SPONSORED CONTENT

Turn collecting

of stop data into an opportunity – not a burden
Save time complying with stop data collection requirements and gather additional insight for agency needs.

FEATURED EDUCATION

University of Cincinnati Online
100% online Bachelor's & Master's in Criminal Justice programs. Learn more!

FEATURED EDUCATION

The Street Officer's Guide to Emergency Medical Tactics
Effectively evaluating and acting quickly with appropriate aid is LIFE SAVING!

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: McCarthy, Steven (POL)
To: Chris Perez
Subject: Re: ALPR & 4RE Decision
Date: Wednesday, March 17, 2021 6:58:33 PM

Thanks Chris.

We will definitely be in touch.

SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Chris Perez <chris.perez@vigilantsolutions.com>
Sent: Wednesday, March 17, 2021 11:22 AM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Kevin Coughlin <KCoughlin@watchguardvideo.com>; Small, Michelle (POL) <Michelle.Small@pol.state.ma.us>; Venkatachalam, Krishna (EPS) <krishna.venkatachalam@mass.gov>; Robles, Francis Jr. (POL) <francis.robles@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>; Ryan Garofano <Ryan.Garofano@motorolasolutions.com>
Subject: ALPR & 4RE Decision

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

Captain McCarthy,

Your email to the group was forwarded over to me from the WatchGuard staff so I just wanted to take a moment to respond. Thanks for meeting my colleague Ryan Garofano yesterday and evaluating the 4RE LPR solution. As you referenced, the field of view for the 4RE is too broad, and asking it to do both LPR + evidence collection has seemed to be a tough ask.

This was the first iteration of the integration we hope to achieve with our partnership with WatchGuard. We are building out a new version of this in the future and this feedback is extremely valuable.

One thing to clarify is that in your email you stated, "What it does underscore is that the Vigilant system needs a purpose-built camera for robust ALPR." I just wanted to note that we do in fact have a series of robust LPR cameras that we've been selling on the market, many of which have been deployed throughout the state of Massachusetts. With your LPR data subscription you'll be able to see both the commercial data ***and*** all of our cameras deployed by

police departments around the country.

I attached some information on our fixed cameras, our solar/quick deploy option, mobile cameras, and mobile app, all of which are integrated into our system. If you're open to further discussions about expanding, want some flexibility, or would like to demo our robust equipment, we would certainly welcome them. I understand you guys have utilized PIPS in the past, but with our recent updates I'm confident you would see an enhancement in both hardware and software functionality. Keep in mind we can always integrate your existing data to avoid having to use 2 separate backends.

If you ever have any questions, please feel free to reach out to either me or Ryan and we'd be happy to discuss.

Happy St. Patty's Day.

Thanks,

Chris Perez
Eastern US Sales Director
Video Security & Analytics
Vigilant Solutions

m: (516) [redacted]
TEMPORARY NUMBER through 3/18 - (242) 824-8837

Grant Assistance | Training | LinkedIn

Support: (925) 398-2079 | Email Support

For more information on how and why we collect your personal information, please visit our Privacy Policy.

From: Cerra, Robert (POL)
To: Cyr, Mark (POL)
Subject: RE: FLOCK nomination process Tweaked
Date: Monday, August 23, 2021 3:59:14 PM

Received Sir
I am in tomorrow

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Monday, August 23, 2021 3:59 PM
To: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Subject: Re: FLOCK nomination process Tweaked

Hi Rob,
Hold off for now. Let's plan to meet quickly on this if you are in the office tomorrow...

Mark

Detective Captain Mark D. Cyr #2728

Massachusetts State Police

Executive Officer

Division of Homeland Security and Preparedness

124 Acton Street

Maynard, MA 01754

508-[redacted] (cell)

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

From: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Sent: Monday, August 23, 2021 3:32 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: FW: FLOCK nomination process Tweaked

Sir,
FLOCK camera systems is looking for success stories for it's automated license plate reader (ALPR)

systems. Gary Ferguson, a dispatcher in A Troop has the blessing of his supervisors up in A Troop to use the systems, according to him. He has been very helpful to us, as well as local law enforcement, in locating vehicles on the system. We wanted to forward this to FLOCK, but wanted to get your approval first.

Respectfully,

Sgt Cerra

Sgt. Robert Cerra #3086
Massachusetts State Police
Commonwealth Fusion Center | Criminal Information Section
124 Acton Street
Maynard, MA 01754
978-451-3777
617-[redacted] (cell)
978-451-3700 (24/7)
The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Neville, Christopher (POL) <Christopher.Neville@pol.state.ma.us>
Sent: Monday, August 23, 2021 1:59 PM
To: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Subject: FW: FLOCK nomination process Tweaked

If you want to put your name ahead of mine on the bottom, please feel free and edit as you see fit.

-

All good cops know that the most important factor in solving crimes is gathering information and using that intelligence to provide leads leading to the identification of suspects. Massachusetts State Police Dispatcher Gary Ferguson works the day shift out of State Police A-Troop Headquarters in Danvers MA. For the past several years, Gary has played a critical role in providing access to photographs of suspect vehicles and criminal intelligence throughout Massachusetts and surrounding states. Gary is always looking for ways to gather intelligence information and took it upon himself to initiate contacts with Metro Boston area Agencies who were using the FLOCK LPR system.

-

Gary's expertise in utilizing the plate readers, and his ability to search for "like" vehicles has uncovered dozens of suspect vehicles and helped to identify just as many suspects.
Recently, the greater Boston area was subjected to Eastern European Traveling criminals who were successful in selling fake gold jewelry, including fake Rolex watches, under the premise of "needing money to get home". Family units comprised of two adults and two young children operating late model SUV rental cars would pull into parking lots, gas stations, or street-side and explain their tale of woe. Victims would be conned into providing as much as $5,000 in cash in exchange for the fake gold jewelry.

In early July, Quincy and Cambridge MA police both received reports of such activity, one of which resulted in the loss of $5,000 to a handicapped individual who was driven to an ATM. Several days later a victim in Malden MA was scammed out of over $3,000 in a gas station parking lot. Using photographs of the encounter in Malden that did NOT show the license plate, Dispatcher Ferguson initiated a review of gray Chevrolet Traverse SUVs that were picked up on Metro-Boston area FLOCK Cameras over the previous week. He reviewed video footage of over a dozen vehicles that matched his search parameters.

Dispatcher Ferguson then compared the Malden surveillance footage with the FLOCK LPR photos and was quickly able to eliminate nine of the vehicles based on roof-rack dissimilarities. Running registration data he determined that three additional vehicles were locally owned by Massachusetts residents in the Boston area and not targets of this investigation, however one out-of-state license plate caught his interest. It was a vehicle owned by a Nationally known Rental Car Company.

Using his years of experience and contacts, he contacted the Security office for the Rental Agency and determined that the vehicle was in-fact recently rented in New York City by an individual of Eastern European nationality. A short time later he was able to determine that the rental vehicle was currently at a gas station in Lexington MA. Shortly thereafter the car was noted to be in a parking lot in Waltham MA. Police responded to that location and found two rental vehicles, side-by-side, both containing Eastern European family units. All parties were identified and photo identifications were obtained. Although probable cause for an arrest was not established at the time, a subsequent photo array conducted by Malden Police resulted in a positive ID by their victim. Malden Police obtained an arrest warrant for that individual. In addition, Waltham police later received a similar fake gold scam report from a victim of the same individual. The suspect soon after dropped the rental car off at LaGuardia Airport in New York.

This story is simply one of many that I am aware of over the past year involving FLOCK cameras being utilized by Dispatcher Ferguson. They range from identifying suspect vehicles involved in the theft of Catalytic Converters in Everett MA, Identifying a suspect and vehicle

involved in a recent conspiracy to steal used vehicles from an Automobile Auction house in Acton, MA, and locating suspect vehicles involved in a wide range of shoplifting , credit card frauds and Organized Retail Crime activity in the Metro Boston area.

I am aware that the State Police are looking into obtaining a new LPR system in an effort to identify and locate criminal suspects, missing and endangered persons and to eliminate potential vehicles from suspicion. Dispatcher Gary Ferguson's reputation for assisting in solving crimes, using your technology, is growing in the New England region and he is certainly one of the individuals who is most responsible for bringing a favorable impression to your product.

As co-administrators of a police information sharing email network with almost 3,000 recipients, it is our pleasure to nominate and recognize someone who takes it upon himself to search for links every day, whether on or off-duty, in an effort to solve crimes, identify suspects, and save hours of investigative time.

Respectfully yours,

J. Christopher Neville
Intelligence Analyst
Commonwealth Fusion Center
Massachusetts State Police
(Det. Lt. Ret. Wilmington MA Police)
macrimenet@pol.state.ma.us
christopher.neville@pol.state.ma.us
Cell 978-[redacted]
Macrimenet@state.ma.us
Sgt. Robert Cerra robert.cerra@pol.state.ma.us c-617-[redacted]
Massachusetts State Police
J. Christopher Neville christopher.neville@pol.state.ma.us c-978-[redacted]
(Det. Lt. Ret. Wilmington MA PD)

From: Cyr, Mark (POL)
To: Cerra, Robert (POL)
Subject: Re: FLOCK nomination process Tweaked
Date: Tuesday, August 24, 2021 1:02:47 PM

---

come down in 5 min

Detective Captain Mark D. Cyr #2728
Massachusetts State Police
Executive Officer
Division of Homeland Security and Preparedness
124 Acton Street
Maynard, MA 01754
508-[redacted] (cell)

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

From: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Sent: Tuesday, August 24, 2021 1:00 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: RE: FLOCK nomination process Tweaked

Good afternoon sir.
I am planning on leaving at 1330 to go to a meeting. If you are not available today, could we try to reschedule for tomorrow?

Respectfully,
Sgt Cerra

From: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Sent: Monday, August 23, 2021 3:59 PM
To: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Subject: Re: FLOCK nomination process Tweaked

Hi Rob,
Hold off for now. Let's plan to meet quickly on this if you are in the office tomorrow...

Mark

Detective Captain Mark D. Cyr #2728
Massachusetts State Police
Executive Officer

Division of Homeland Security and Preparedness
124 Acton Street
Maynard, MA 01754
508-[redacted] (cell)

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

From: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Sent: Monday, August 23, 2021 3:32 PM
To: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: FW: FLOCK nomination process Tweaked

Sir,
FLOCK camera systems is looking for success stories for it's automated license plate reader (ALPR) systems. Gary Ferguson, a dispatcher in A Troop has the blessing of his supervisors up in A Troop to use the systems, according to him. He has been very helpful to us, as well as local law enforcement, in locating vehicles on the system. We wanted to forward this to FLOCK, but wanted to get your approval first.

Respectfully,

Sgt Cerra

Sgt. Robert Cerra #3086
Massachusetts State Police
Commonwealth Fusion Center | Criminal Information Section
124 Acton Street
Maynard, MA 01754
978-451-3777
617-[redacted] (cell)
978-451-3700 (24/7)
The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Neville, Christopher (POL) <Christopher.Neville@pol.state.ma.us>
Sent: Monday, August 23, 2021 1:59 PM

To: Cerra, Robert (POL) <robert.cerra@pol.state.ma.us>
Subject: FW: FLOCK nomination process Tweaked

If you want to put your name ahead of mine on the bottom, please feel free and edit as you see fit.

-
All good cops know that the most important factor in solving crimes is gathering information and using that intelligence to provide leads leading to the identification of suspects. Massachusetts State Police Dispatcher Gary Ferguson works the day shift out of State Police A-Troop Headquarters in Danvers MA. For the past several years, Gary has played a critical role in providing access to photographs of suspect vehicles and criminal intelligence throughout Massachusetts and surrounding states. Gary is always looking for ways to gather intelligence information and took it upon himself to initiate contacts with Metro Boston area Agencies who were using the FLOCK LPR system.
-
Gary's expertise in utilizing the plate readers, and his ability to search for "like" vehicles has uncovered dozens of suspect vehicles and helped to identify just as many suspects. Recently, the greater Boston area was subjected to Eastern European Traveling criminals who were successful in selling fake gold jewelry, including fake Rolex watches, under the premise of "needing money to get home". Family units comprised of two adults and two young children operating late model SUV rental cars would pull into parking lots, gas stations, or street-side and explain their tale of woe. Victims would be conned into providing as much as $5,000 in cash in exchange for the fake gold jewelry.

In early July, Quincy and Cambridge MA police both received reports of such activity, one of which resulted in the loss of $5,000 to a handicapped individual who was driven to an ATM. Several days later a victim in Malden MA was scammed out of over $3,000 in a gas station parking lot. Using photographs of the encounter in Malden that did NOT show the license plate, Dispatcher Ferguson initiated a review of gray Chevrolet Traverse SUVs that were picked up on Metro-Boston area FLOCK Cameras over the previous week. He reviewed video footage of over a dozen vehicles that matched his search parameters.

Dispatcher Ferguson then compared the Malden surveillance footage with the FLOCK LPR photos and was quickly able to eliminate nine of the vehicles based on roof-rack dissimilarities. Running registration data he determined that three additional vehicles were locally owned by Massachusetts residents in the Boston area and not targets of this investigation, however one out-of-state license plate caught his interest. It was a vehicle owned by a Nationally known Rental Car Company.

Using his years of experience and contacts, he contacted the Security office for the Rental Agency and determined that the vehicle was in-fact recently rented in New York City by an

individual of Eastern European nationality. A short time later he was able to determine that the rental vehicle was currently at a gas station in Lexington MA. Shortly thereafter the car was noted to be in a parking lot in Waltham MA. Police responded to that location and found two rental vehicles, side-by-side, both containing Eastern European family units. All parties were identified and photo identifications were obtained. Although probable cause for an arrest was not established at the time, a subsequent photo array conducted by Malden Police resulted in a positive ID by their victim. Malden Police obtained an arrest warrant for that individual. In addition, Waltham police later received a similar fake gold scam report from a victim of the same individual. The suspect soon after dropped the rental car off at LaGuardia Airport in New York.

This story is simply one of many that I am aware of over the past year involving FLOCK cameras being utilized by Dispatcher Ferguson. They range from identifying suspect vehicles involved in the theft of Catalytic Converters in Everett MA, Identifying a suspect and vehicle involved in a recent conspiracy to steal used vehicles from an Automobile Auction house in Acton, MA, and locating suspect vehicles involved in a wide range of shoplifting , credit card frauds and Organized Retail Crime activity in the Metro Boston area.

I am aware that the State Police are looking into obtaining a new LPR system in an effort to identify and locate criminal suspects, missing and endangered persons and to eliminate potential vehicles from suspicion. Dispatcher Gary Ferguson's reputation for assisting in solving crimes, using your technology, is growing in the New England region and he is certainly one of the individuals who is most responsible for bringing a favorable impression to your product.

As co-administrators of a police information sharing email network with almost 3,000 recipients, it is our pleasure to nominate and recognize someone who takes it upon himself to search for links every day, whether on or off-duty, in an effort to solve crimes, identify suspects, and save hours of investigative time.

Respectfully yours,

J. Christopher Neville
Intelligence Analyst
Commonwealth Fusion Center
Massachusetts State Police
(Det. Lt. Ret. Wilmington MA Police)
macrimenet@pol.state.ma.us
christopher.neville@pol.state.ma.us
Cell 978-[redacted]
Macrimenet@state.ma.us
Sgt. Robert Cerra robert.cerra@pol.state.ma.us c-617-[redacted]

Massachusetts State Police
J. Christopher Neville *christopher.neville@pol.state.ma.us* *c-978-*[redacted]
(Det. Lt. Ret. Wilmington MA PD)

From: Egnitz, Brian (POL)
To: Schwarz, William J
Cc: Cochrane, William
Subject: RE: lpr help
Date: Tuesday, September 7, 2021 8:06:00 AM

Hi Bill,

Thank you for reaching out. This is the latest that I have on the ALPR system;

- EOTSS has purchased 3 years of cloud storage for all existing cameras
- EOPSS/EOTSS are working through logistics of migrating hot files to the Neology cloud
- EOPSS/EOTSS/MSP are working through offloading the 2019 preserved data to the cloud with the vendor.

MSP also wants the system back online, we are pushing to have the system up for the marathon as we leverage ALPR for security. That said, MSP does not own the system and are not in control of the timeline.

-Brian

From: Schwarz, William J <WSchwarz@springfieldpolice.net>
Sent: Wednesday, September 1, 2021 10:21 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Cochrane, William <WCochrane@springfieldpolice.net>
Subject: lpr help

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

Sir;

I hope this email finds you well. Deputy Cochrane has been tasked with our recent uptick in Drag Racing here in Springfield. In doing our enforcement details over the past 3 weeks it has become glaringly obvious that this is a regional problem. We have planned a regional approach for the coming weekend nights to include MSP, West Springfield and Chicopee PD support. The operation would be greatly enhanced by having access to License plate readers. We recognize that you has been working diligently to get the system up and running, and have been receptive to any questions relating to same. Can you give us any timeline or help with this? Any help would be greatly appreciated.

Bill

William Schwarz

Director of Crime Analysis / Real Time Analysis Center
130 Pearl St.
Springfield, MA 01105
413-886-5282

From: Pack, Noah (POL)
To: Craig Lynch
Subject: Re: MOU and Axon Promo - Flock Safety
Date: Tuesday, December 7, 2021 9:04:48 PM

Hi Craig,

I am setting up a meeting with our legal section regarding a number of issues, to include the Flock MOU and nationwide study/trial program. I expect to be asked for the fine print on the study, including what are we expected to do with our participation, what happens to the data, etc. Can you provide any further info on that?

Respectfully,

Noah

Sergeant Noah H. Pack
Massachusetts State Police
Division of Homeland Security and Preparedness
Office of the Division Commander
470 Worcester Road
Framingham, Massachusetts 01702

From: Craig Lynch <craig.lynch@flocksafety.com>
Sent: Wednesday, December 1, 2021 9:16 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: MOU and Axon Promo - Flock Safety

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

Sgt Pack - Nice speaking with you this morning. I have attached the Flock Safety MOU which will give access to everything in the system as a paying custom other than the NationWide Search of ~9500 cameras.

Below is the email with details on the Axon promotion. It's a bit lengthy, but 1 year, no obligation, no multi-year commitment.

As Axon Founder and CEO Rick Smith announced at the MCSA Fall Meeting, Axon along with its partner Flock Safety, will provide all MCSA agencies Automated License Plate Readers (ALPR) for one year for those willing to participate in a national study conducted by the Police Foundation. While many recognize the crime-reduction benefits of ALPR technology, questions have been raised about how effective they are at reducing all crime types as well the civil liberties and privacy implications of this technology. This study will attempt to provide a robust research design and methodology to address those questions and

concerns.

If your agency is willing to take part in this national study, you will receive:

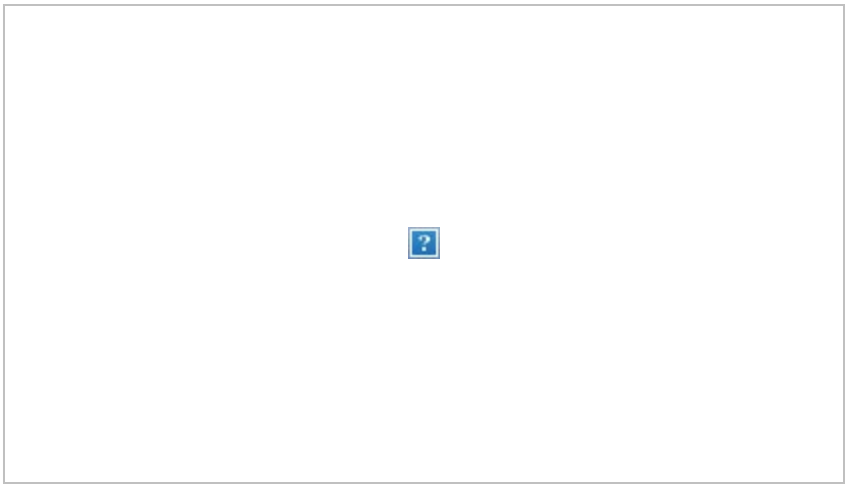
- **25 Flock Safety ALPRs for 1 year, which includes the ALPR readers, solar or DC power, mounting equipment, and installation.**
- **This also includes all cloud hosting and analytics, including LTE connectivity, unlimited licenses, hotlist integration and alerts, and ongoing software enhancements.**
- **Flock Safety will make their SMEs available to assist agencies with identifying the most effective ALPR locations.**
- **Agencies can purchase additional cameras beyond the 25. Axon and Flock will cover the installation costs of these additional cameras.**
- **This offer applies to any MCSA agency, including those that have already purchased Flock ALPRs.**
- **After the 1-year field trial offer ends, each agency has the option to purchase the units at $2500 per year per ALPR.**
- **Should an agency choose not to retain the ALPRs after the field trial, we will ensure that the agency is able to transfer their data to another system and we will remove the ALPRs at no cost to the agency.**

In addition, we understand that across the country there are varying laws and regulations about ALPR technology. Axon's Government Affairs team will be available to your agency to provide an overview of any state and county ALPR laws that are applicable. We will also provide model ALPR policies to your agency prior to deployment. And, our Government Affairs team can act as a resource to meet with and educate any county board member(s) on Axon, Flock Safety, ALPR technology — and our ethics-first design philosophy.

If you or your team have any questions, please let me know.

Thanks for your partnership,

Craig
--



From: Craig Lynch
To: Pack, Noah (POL)
Subject: Re: MOU and Axon Promo - Flock Safety
Date: Tuesday, December 7, 2021 9:35:25 PM

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

Sgt - I have a high level idea on this but I don't want to waste your time. I sent your request over to my good buddy who works for Flock and manages the Axon relationship. I hope to have some info tonight or early tomorrow and I'll shoot it over to you.

Best,

Craig

On Tue, Dec 7, 2021 at 9:04 PM Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

> Hi Craig,
>
> I am setting up a meeting with our legal section regarding a number of issues, to include the Flock MOU and nationwide study/trial program. I expect to be asked for the fine print on the study, including what are we expected to do with our participation, what happens to the data, etc. Can you provide any further info on that?
>
> Respectfully,
>
> Noah
>
> **Sergeant Noah H. Pack**
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> Office of the Division Commander
> 470 Worcester Road
> Framingham, Massachusetts 01702
>
> ---
>
> **From:** Craig Lynch <craig.lynch@flocksafety.com>
> **Sent:** Wednesday, December 1, 2021 9:16 AM
> **To:** Pack, Noah (POL) <noah.pack@pol.state.ma.us>
> **Subject:** MOU and Axon Promo - Flock Safety
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Sgt Pack - Nice speaking with you this morning. I have attached the Flock Safety MOU

which will give access to everything in the system as a paying custom other than the NationWide Search of ~9500 cameras.

Below is the email with details on the Axon promotion. It's a bit lengthy, but 1 year, no obligation, no multi-year commitment.

As Axon Founder and CEO Rick Smith announced at the MCSA Fall Meeting, Axon along with its partner Flock Safety, will provide all MCSA agencies Automated License Plate Readers (ALPR) for one year for those willing to participate in a national study conducted by the Police Foundation. While many recognize the crime-reduction benefits of ALPR technology, questions have been raised about how effective they are at reducing all crime types as well the civil liberties and privacy implications of this technology. This study will attempt to provide a robust research design and methodology to address those questions and concerns.

If your agency is willing to take part in this national study, you will receive:

- **25 Flock Safety ALPRs for 1 year, which includes the ALPR readers, solar or DC power, mounting equipment, and installation.**
- **This also includes all cloud hosting and analytics, including LTE connectivity, unlimited licenses, hotlist integration and alerts, and ongoing software enhancements.**
- **Flock Safety will make their SMEs available to assist agencies with identifying the most effective ALPR locations.**
- **Agencies can purchase additional cameras beyond the 25. Axon and Flock will cover the installation costs of these additional cameras.**
- **This offer applies to any MCSA agency, including those that have already purchased Flock ALPRs.**
- **After the 1-year field trial offer ends, each agency has the option to purchase the units at $2500 per year per ALPR.**
- **Should an agency choose not to retain the ALPRs after the field trial, we will ensure that the agency is able to transfer their data to another system and we will remove the ALPRs at no cost to the agency.**

In addition, we understand that across the country there are varying laws and regulations about ALPR technology. Axon’s Government Affairs team will be available to your agency to provide an overview of any state and county ALPR laws that are applicable. We will also provide model ALPR policies to your agency prior to deployment. And, our Government Affairs team can act as a resource to meet with and educate any county board member(s) on Axon, Flock Safety, ALPR technology — and our ethics-first design philosophy.

If you or your team have any questions, please let me know.

Thanks for your partnership,

Craig

--



This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

--



From: NFCA President
Subject: Register Now for Tuesday and Wednesday Presentations by Cobwebs Technologies and CODY Systems
Date: Monday, September 20, 2021 6:51:25 PM

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

NFCA Sponsor Education Series sessions are offered at 1:00 pm EST on Tuesday and Wednesday this week. Details and registration links for presentations by Cobwebs Technologies and CODY Systems are below.

Tuesday, September 21: Cobwebs Technologies

Mitigating Threats in Real-time

Please join us on Tuesday, September 21, 2021 1pm EST to discuss methodologies used to identify and mitigate threats through open-source investigations. We will showcase how to access the deep web to detect and assess threats made against people, property, and government and how automated systems can allow you to become much more effective in tie-sensitive matters. During this session, you will acquire knowledge on how to apply best practices to assess what threats matter to you and your agency, all in real-time.

Our host Allison Sullivan is a Web Intelligence Analyst, who brings 17 years of law enforcement experience as a crime and intelligence analyst.

Register here:

Mitigating Threats in real time

Wednesday, September 22: CODY System

COBRAnet: Fusion Center Fuel for Real-time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data interoperability technology fuels fusion centers with a one-stop real-time search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider, while providing an independent data foundation for all data-driven fusion center missions.

Register here:

CODY Systems: COBRAnet: Fusion Center Fuel for Real-time Data Interoperability

Thank you for participating in the Sponsor Education Series.

From: NFCA President
Subject: Register Now for Tuesday and Wednesday Presentations by Cobwebs Technologies and CODY Systems
Date: Monday, September 20, 2021 6:49:46 PM

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

NFCA Sponsor Education Series sessions are offered at 1:00 pm EST on Tuesday and Wednesday this week. Details and registration links for presentations by Cobwebs Technologies and CODY Systems are below.

Tuesday, September 21: Cobwebs Technologies

Mitigating Threats in Real-time

Please join us on Tuesday, September 21, 2021 1pm EST to discuss methodologies used to identify and mitigate threats through open-source investigations. We will showcase how to access the deep web to detect and assess threats made against people, property, and government and how automated systems can allow you to become much more effective in tie-sensitive matters. During this session, you will acquire knowledge on how to apply best practices to assess what threats matter to you and your agency, all in real-time.

Our host Allison Sullivan is a Web Intelligence Analyst, who brings 17 years of law enforcement experience as a crime and intelligence analyst.

Register here:

Mitigating Threats in real time

Wednesday, September 22: CODY System

COBRAnet: Fusion Center Fuel for Real-time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data interoperability technology fuels fusion centers with a one-stop real-time search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider, while providing an independent data foundation for all data-driven fusion center missions.

Register here:

CODY Systems: COBRAnet: Fusion Center Fuel for Real-time Data Interoperability

Thank you for participating in the Sponsor Education Series.

From: NFCA President
Subject: Register Now for Tuesday and Wednesday Presentations by Cobwebs Technologies and CODY Systems
Date: Monday, September 20, 2021 6:53:08 PM

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

NFCA Sponsor Education Series sessions are offered at 1:00 pm EST on Tuesday and Wednesday this week. Details and registration links for presentations by Cobwebs Technologies and CODY Systems are below.

Tuesday, September 21: Cobwebs Technologies

Mitigating Threats in Real-time

Please join us on Tuesday, September 21, 2021 1pm EST to discuss methodologies used to identify and mitigate threats through open-source investigations. We will showcase how to access the deep web to detect and assess threats made against people, property, and government and how automated systems can allow you to become much more effective in tie-sensitive matters. During this session, you will acquire knowledge on how to apply best practices to assess what threats matter to you and your agency, all in real-time.

Our host Allison Sullivan is a Web Intelligence Analyst, who brings 17 years of law enforcement experience as a crime and intelligence analyst.

Register here:

Mitigating Threats in real time

Wednesday, September 22: CODY System

COBRAnet: Fusion Center Fuel for Real-time Data Interoperability

Wasting valuable time navigating through multiple different systems in order to gather intel? COBRAnet data interoperability technology fuels fusion centers with a one-stop real-time search across all the distinct systems they rely on (IMS/CMS, RMS, JMS, ALPR, etc.) regardless of system provider, while providing an independent data foundation for all data-driven fusion center missions.

Register here:

CODY Systems: COBRAnet: Fusion Center Fuel for Real-time Data Interoperability

Thank you for participating in the Sponsor Education Series.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Riots in Portland over Minn OIS; Biden picks Tucson chief to lead CBP
Date: Tuesday, April 13, 2021 4:13:05 PM

April 13, 2021 | View as webpage

Dear Police1 Member,

Tactics keep you alive, but report writing keeps you out of trouble, something most agencies dismiss as an important officer survival skill.

In tomorrow's Careers eNewsletter we share he three techniques that will instantly improve your report writing, avoid case dismissal and protect yourself as an officer.

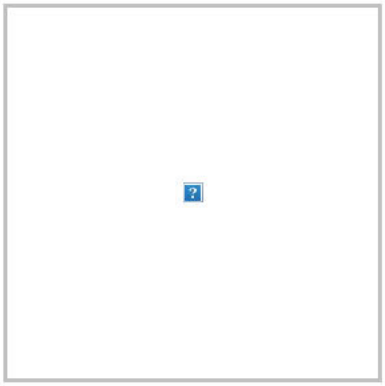
PLUS: 12 things to consider before making a lateral transfer.

Sign up today to ensure you receive a copy of the newsletter in your inbox tomorrow.

Stay safe,

— The Police1 Team

TOP STORIES



Unrest continues after chief says officer meant to use TASER; 40 arrested

Hundreds defied curfew during the second night of tensions in a Minneapolis suburb

Miss. deputy killed in crash

Biden to pick Tucson police chief to lead Customs and Border Protection

Portland PD declares riot as crowd protests Daunte Wright OIS

2nd Capitol officer slain this year to lie in honor Tuesday

NM governor signs bill to legalize recreational pot

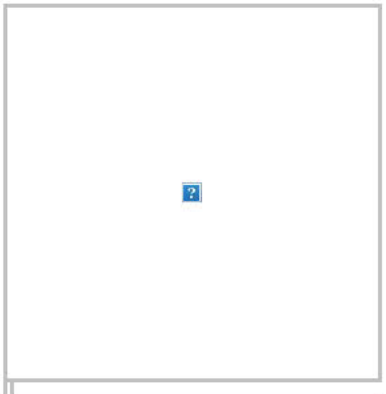
SRO shot at Tenn. high school recovering

COMMAND LIGHT RELEASES LAW ENFORCEMENT CATALOG



See the Command C-Lite in ac ion, featuring spotlight/floodlight combo, 120-degree tilt and optional rota ion.

See it in action



#TRAININGTUESDAY



6 simple skills officers need to

prevail in a fight

By Todd Fletcher

It's incumbent upon officers to overcome a resistant suspect quickly to minimize the risk of injury to everyone

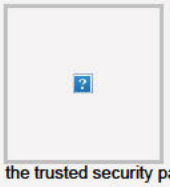


Be tactically proactive not just reactive

By Lt. Dan Marcou

Follow this philosophy whether responding to a riot or supporting a search warrant

Life After Law Enforcement



Put your knowledge and reputa ion into action hrough business ownership in the security industry. Surveillance Secure trains you to become the trusted security partner for businesses in your community.

Request information today

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

VERBAL COMMUNICATION SKILLS



Effective verbal communication in use of force situations

By Tyson Kilbey

Defensive tactics skills and verbal communication skills should not be an either/or option



Why loud & repetitive verbal commands can hinder compliance

By Duane Wolfe

Using loud, repetitive verbal commands can be more of a hindrance than a help when trying to gain compliance from a resis ive subject



SPONSORED CONTENT



How 'green cameras' can improve more than just traffic safety

ALPR-integrated cameras paired with data analysis software can police criminal activity, as well as manage hazardous

greenhouse
gases.

FEATURED EDUCATION



Develop Your Leadership Skills
Join 850+ LE leaders in this nationally-ranked program. 100% online. Learn more today.

FEATURED PRESS RELEASE



How To Buy Online Training Systems
Download this Police1 buying guide

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click **here to unsubscribe.** Visit our **Customer Support** page to report any email problems or **subscribe to our other newsletters.**

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Axon Roadshow
To: McCarthy, Steven (POL)
Subject: Roll on over to our Roadshow to see Fleet 3!
Date: Tuesday, October 12, 2021 11:12:22 AM

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

Axon

banner alt text

Hi Steven,

The 2021 Axon Roadshow is coming to a city near you with free lunch and swag!

There's a lot to see at the roadshow, so can we suggest you start with checking out Axon Fleet 3, our new and most powerful in-car camera? You'll learn about:

- A powerful, reliable dual-view camera with clear panoramic views
- An integrated 4K ALPR camera that can cover three traffic lanes
- Real-time situational awareness features including live alerts, maps, and streaming

Check out the roadshow stops near you and register today.

REGISTER NOW

We hope to see you there!

- The Axon Team

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The Delta Logo, Axon, and Axon Citizen are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information visit www.axon.com/legal.

All Rights Reserved. © 2021 Axon Enterprise, Inc.

Privacy Policy

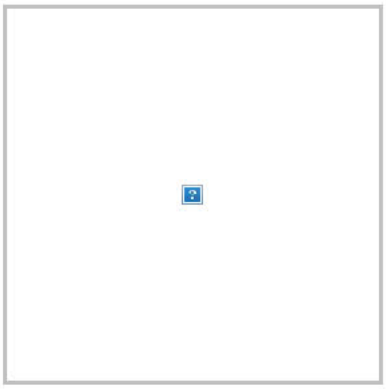
Contact Us

Unsubscribe

From: Police1 Roll Call
To: zzNee William (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:06:21 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

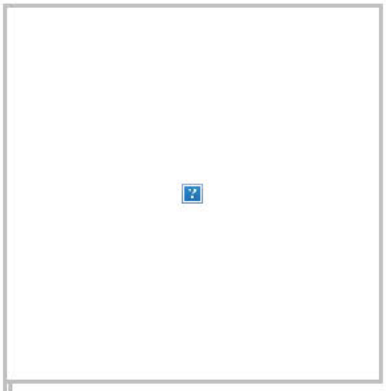
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

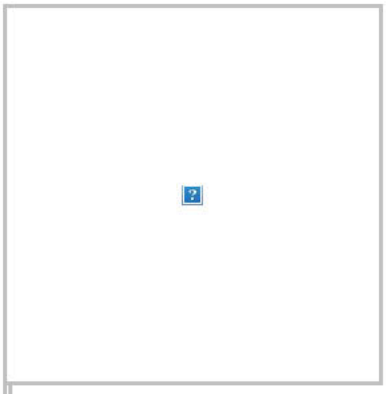


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



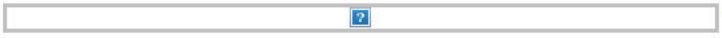
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

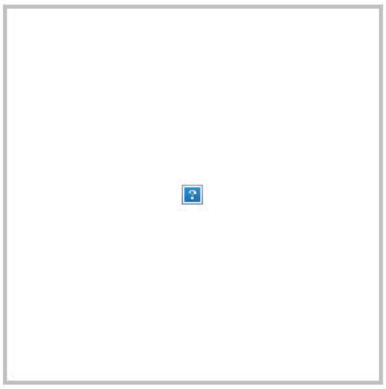
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Clement_Michael (POL)
Subject: Sacramento"s "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:06:00 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

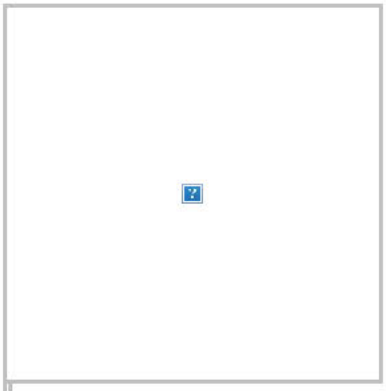
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience



What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation

Improve Efficiency With Mobile ALPR

Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

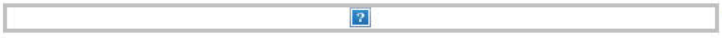


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

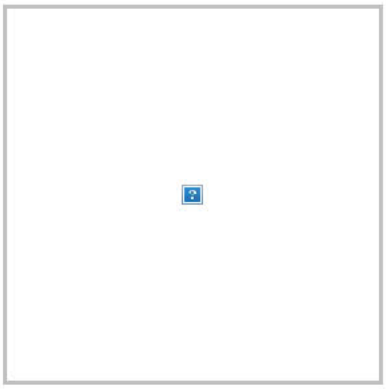
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:05:26 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

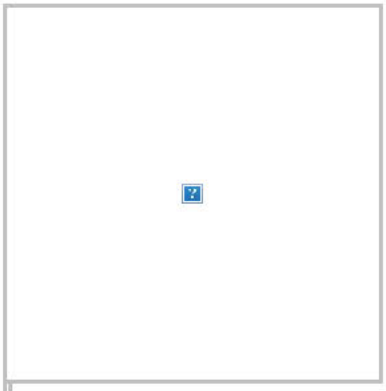
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

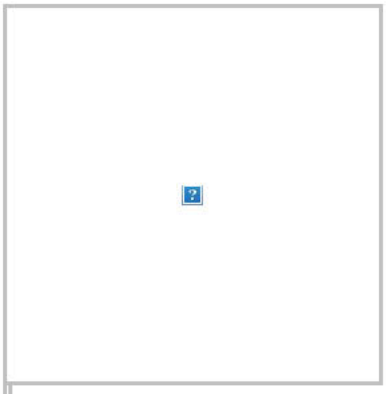


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

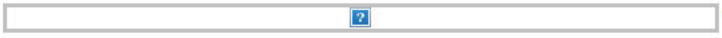


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

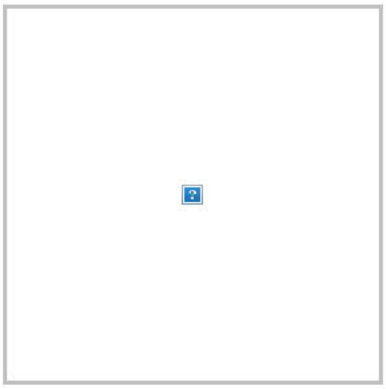
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lawlor Jr Daniel (POL)
Subject: Sacramento"s "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:04:50 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

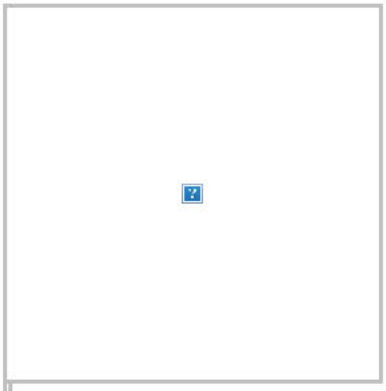
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

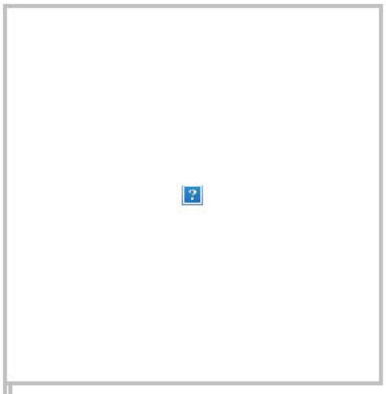


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

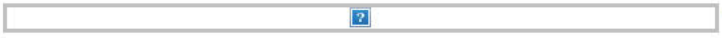


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

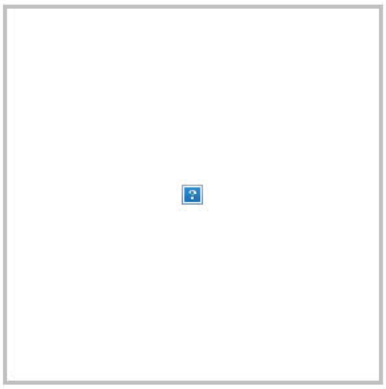
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Irwin Patrick (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:04:17 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

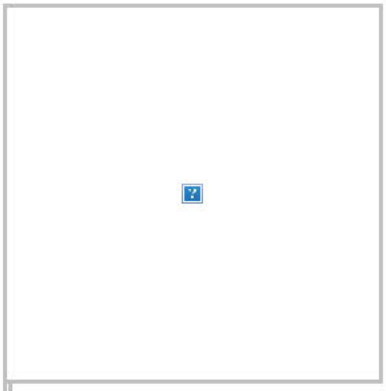
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

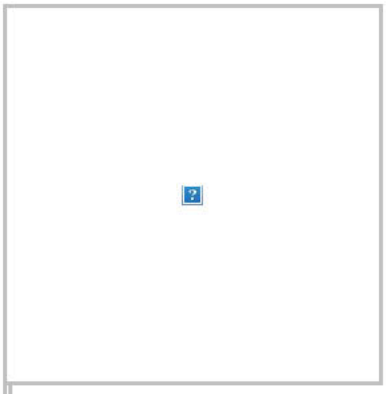


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

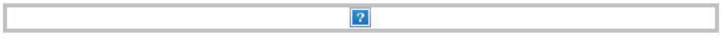


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

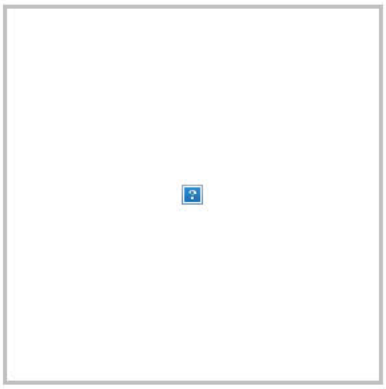
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Tulipano, Michael (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:03:07 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

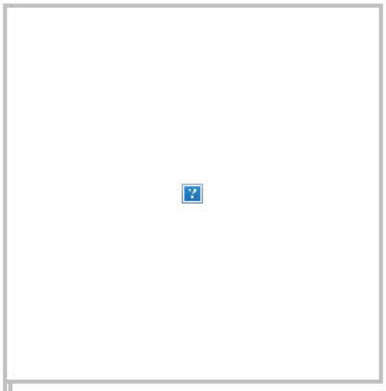
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT

A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

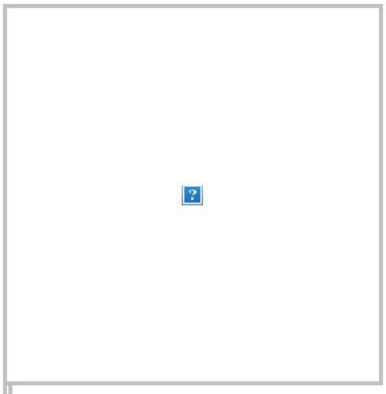
When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

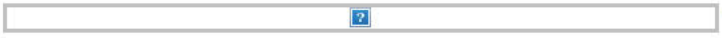


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

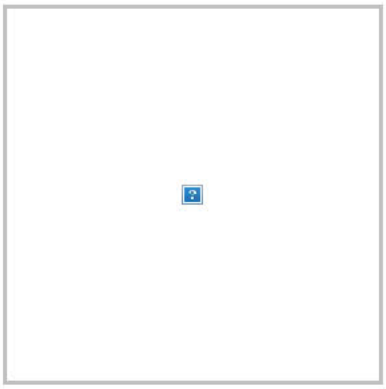
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lavoie_Marc (POL)
Subject: Sacramento"s "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:02:52 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

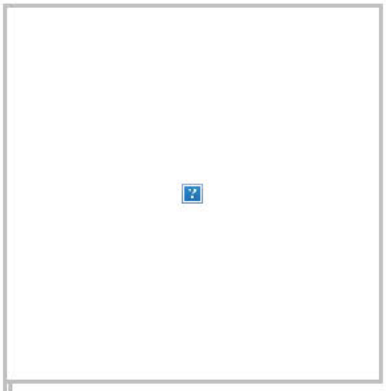
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT

A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

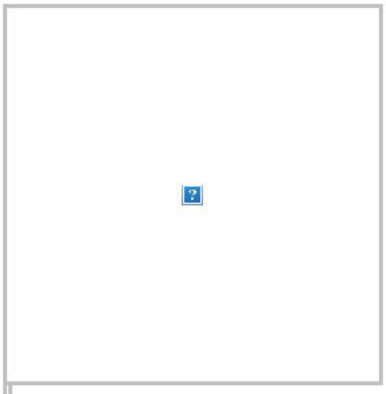
When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

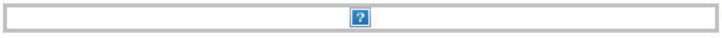


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

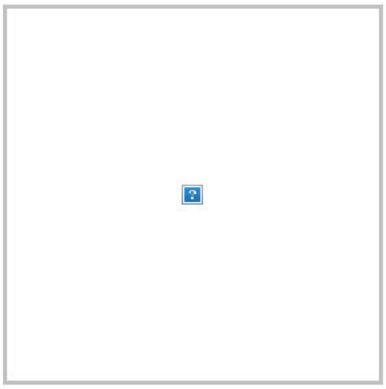
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Mcginn_Daniel (POL)
Subject: Sacramento"s "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:02:28 PM

August 16, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

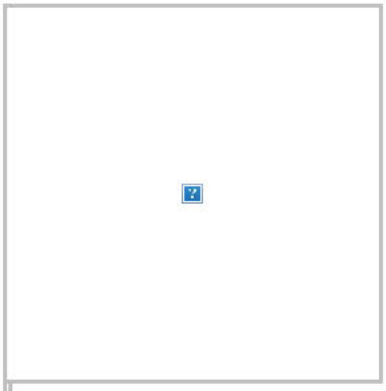
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

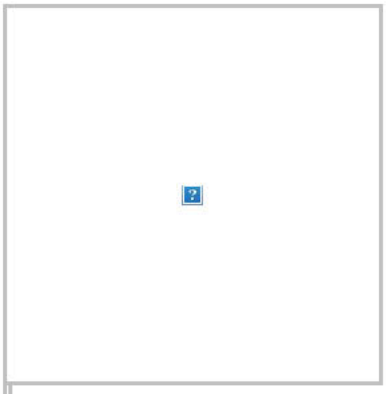


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



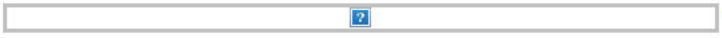
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

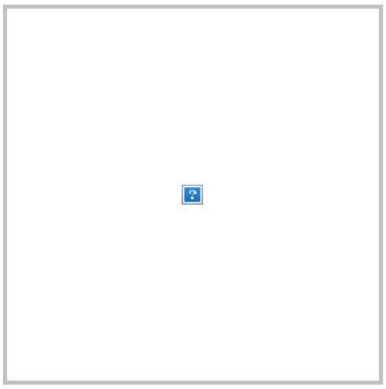
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Rizos, Byron (POL)
Subject: Sacramento"s "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 2:13:43 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

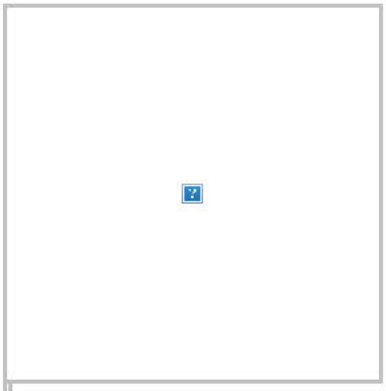
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT

A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

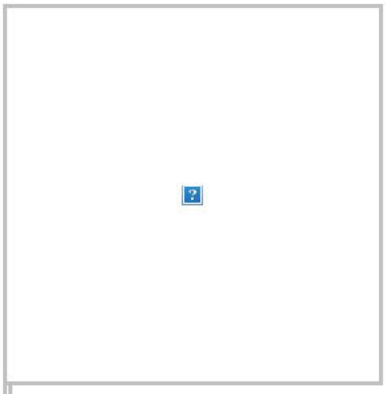
When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

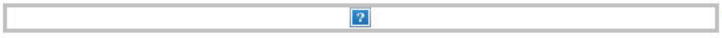


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

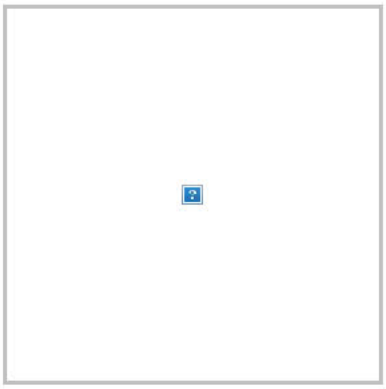
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cooper, Brian (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 2:09:06 PM

August 16, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

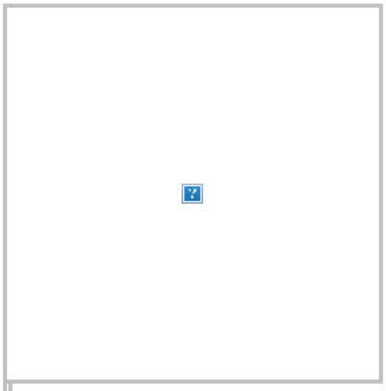
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT

A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

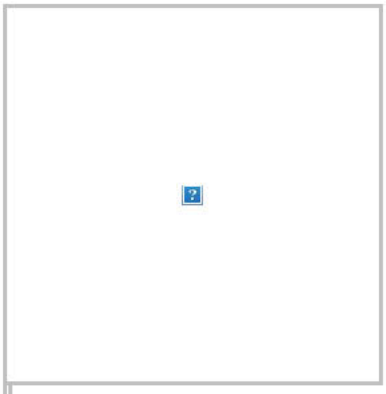
When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



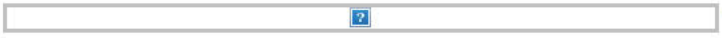
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

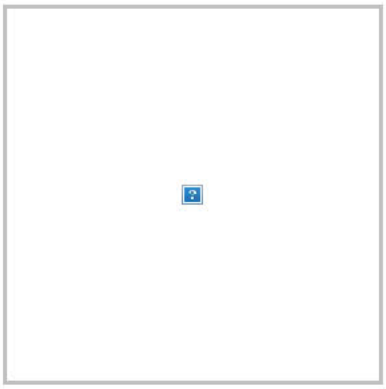
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Paquette, Brian (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 2:08:12 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

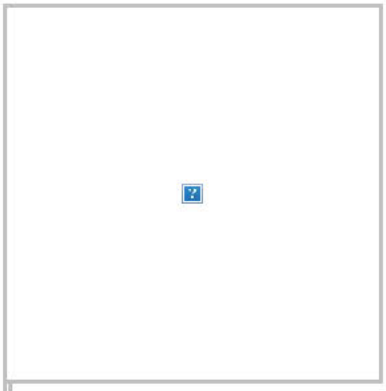
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

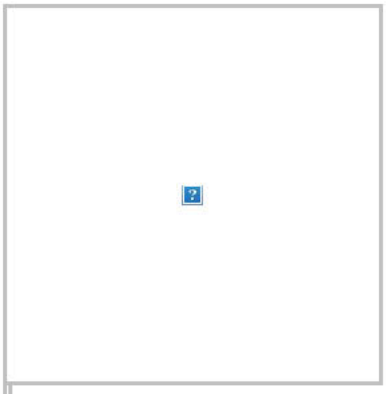


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



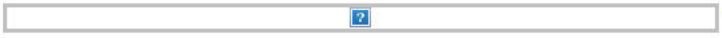
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

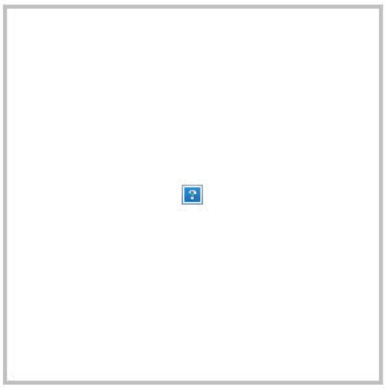
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cronin, John E (POL)
Subject: Sacramento"s "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 2:07:38 PM

August 16, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

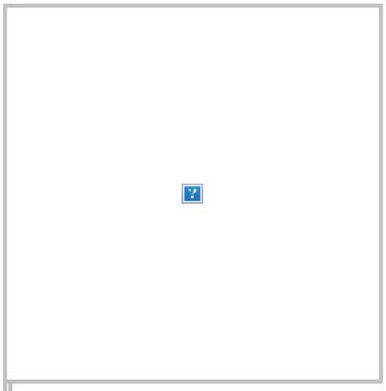
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT

A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

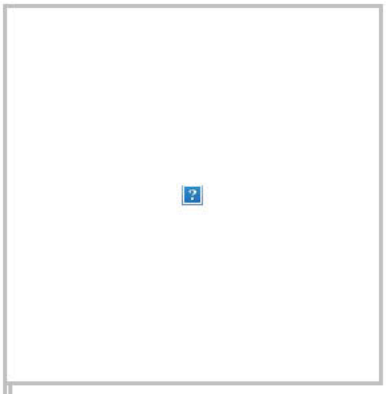
When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur

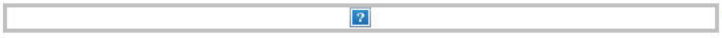


5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years

SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.

FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

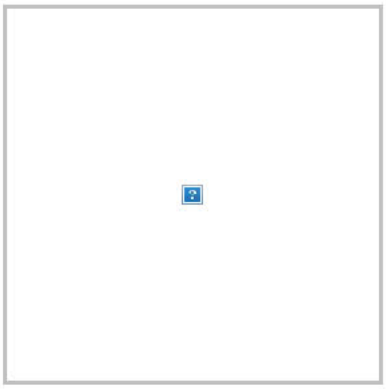
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzJoyce, Gina (POL)
Subject: Sacramento's "vaccinate or terminate" policy; Cop saves 9 lives in rookie year
Date: Monday, August 16, 2021 5:08:30 PM

August 16, 2021 | View as webpage | **Too many emails?** Update Subscription Preferences

TOP STORIES



Rookie D.C. cop commended for saving 9 lives in first year on the job

Taylor Brandt credits her tactical emergency medical training from the department for being able to give nine people another chance at life

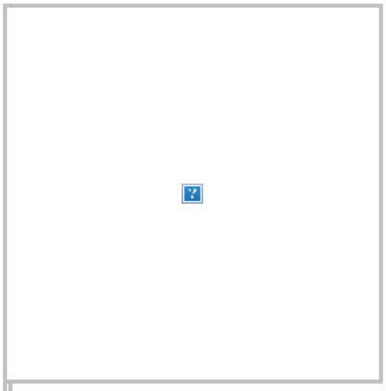
N.C. police officer dies after responding to house fire

Mich. deputy dies after being shot during pursuit

Calif. capital to require all city employees to get vaccinated or face discipline

Minneapolis mayor unveils plan to boost police funding closer to previous levels

'I'm just like everybody else': N.C. deputy chasing NASCAR dream



A Load-Bearing Vest That Offers Protection in a Uniform Look



This neat and discreet plate carrier and vest offers body armor protection while lessening the strain on your back.

Lighten your load

FEATURED CONTENT



A letter to the American public: Law enforcement officers cannot read minds

By Kyle Sumpter

When asked to predict an assailant's intent, officers can only guess, based on articulable observations compared with experience

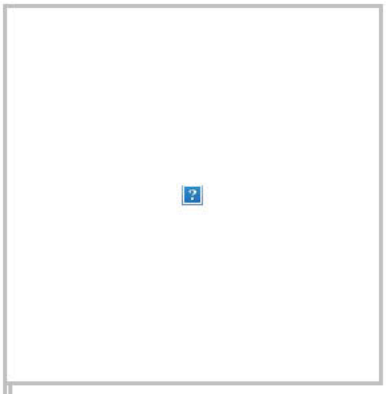


What does it mean to win an encounter?

By Lyons Hale

If we can manage our own emotions by understanding how an irate person affects us, we can

remain calm in the face of provocation



Improve Efficiency With Mobile ALPR



Learn how highly advanced mobile ALPR technology with powerful AI software greatly enhances your department's efficiency and saves on ime and resources.

Learn more

INCEL AWARENESS



The violent fringe of the incel movement

By Dean C. Alexander and Dominic Lesniewski

Raising awareness about the incel movement could help prevent acts of mass violence before they occur



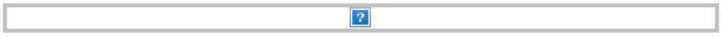
5 things to know about incels

By Police1 Staff

Incels have been linked to multiple acts of mass violence over the past few years



SPONSORED CONTENT



Webinar: How to deploy critical communications

On August 24, find out how LMR and Wireless WAN technologies provide law enforcement agencies the services, information and correspondence they need to make informed decisions and act quickly.



FEATURED JOB



MPD Entry-Level & Reserve Officer Positions Available - Apply Today!

Apply now

FEATURED VIDEO



7 things to look for in an in-car video system

Find out how to choose a system that's right for your department.

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

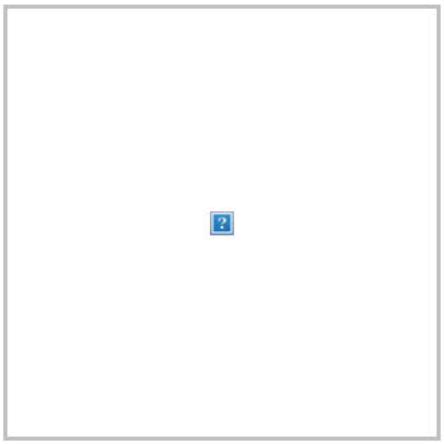
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: School bus hijacked by armed army recruit; Zoo cancels "divisive" police event
Date: Thursday, May 6, 2021 5:15:09 PM

May 6, 2021 | View as webpage

TOP STORIES



Shooting at Idaho middle school injures 3; student captured

The victims' injuries were not believed to be life-threatening, the sheriff said

Army trainee armed with rifle hijacks bus with elementary school children aboard

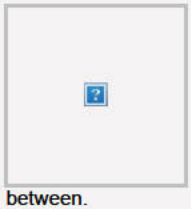
Suspect in shooting of off-duty LAPD cop had been arrested twice in past 3 months

Ala. PD releases bodycam video of fatal OIS

New Orleans zoo cancels pro-police promotion, citing 'divisive' potential

Calif. police officers fight to keep girls off the streets with kickboxing

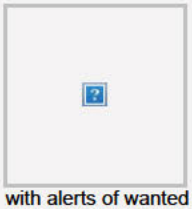
AppTrac-365: Officer Visibility Made Affordable



Every call is a risk. AppTrac-365 gives your agency real-time vis bility of your team - whether serving a warrant, on traffic patrol, or anything in between.

Protect your team today

Catch More Criminals With Rekor ALPR!



Rekor's AI-powered license plate recognition software scans plates and compares them to hotlists providing law enforcement officers with alerts of wanted vehicles.

Learn more

FEATURED CONTENT



State your case: Should the NYPD have returned its robot dog?

By Jim Dudley & Chief Joel Shults, EdD

Following the deployment of a robotic K-9 in

February 2021, public backlash led the NYPD to send 'Digidog' back to the doghouse

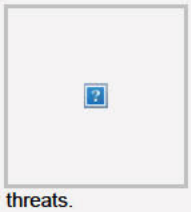


Can coaching be beneficial in policing?

By Obed Magny

Utilizing coaches could lead to higher job satisfaction, better retention, increased trust with community members and increased officer safety

Why Police Should Approach Training as a Continuum of Learning (eBook)



Download this free eBook to learn how virtual training, live fire and shoot house training are converging to prepare today's officers for tomorrow's threats.

Download now

How Does Your Agency Handle Facial Identification?



Police1 wants to know how law enforcement agencies are handling facial identification today, from training to technology. Share your thoughts in our 3-minute survey for a chance to win one of five $100 Amazon gift cards.

Start the survey

LATERAL TRANSFERS



Finding success as a lateral officer

By Andrew Heuett

Step in the door on day one with humility and an attitude that convinces your new agency you have the intent to learn and work hard



2 questions to ask before switching police departments

By Jason Hoschouer

There are many reasons a police officer may decide to move between agencies, but what should you consider before changing departments?



SPONSORED CONTENT



Who'll have your back if you use lethal force in self-defense?

A legal service plan can protect you and your family in a self-defense case.



FEATURED VIDEO



3D SWAT Targets from Dummies Unlimited

Watch the video

FEATURED PRESS RELEASE



How To Buy Online Training Systems

Download the guide

FEATURED COMPANY NEWS

SENTRY Solutions' dry lubrication system cleans and protects while using your firearms and knives



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco,

TX 75034.

From: Joel Griffin, Editor, SecurityInfoWatch.com
To: Crouse, David (POL)
Subject: Security Frontline: The new paradigm in stadium security, Maintaining cybersecurity for remote work post-pandemic, more
Date: Tuesday, August 17, 2021 3:28:02 PM

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

Security Frontline E-Newsletter | View online

Security Frontline E-Newsletter

August 17, 2021

FEATURED STORY

Auburn Nov 2019Christopher Kinnan,IIFX

Security Challenges Await as Football Fans Return to Stadiums

By Steve Lasky

Both college and professional venues prepare for a season of risk unlike any other

How Campus Security Is Being Redefined

Ste Connect Dormakaba August21

From dormakaba USA

Check out this edition of STE Connect to learn how the Covid-19 pandemic and other trends are altering the security landscape today in both K-12 and higher education institutions

Click Here to Continue Reading

TOP NEWS

The New Normal and a Safe Return to School

School safety and security officials must have a crisis plan and a will to implement it

Student dead, another in custody, following shooting at N.M. middle school

No other injuries reported, police investigating motive

The 'new normal' for cybersecurity

Organizations must learn how to safely accommodate remote work trends beyond the pandemic

Texas law will block IT contracts with some foreign vendors

Legislation designed to protect state's critical infrastructure

T-Mobile probing claims of data breach of 100 million customers in U.S.

Compromised data reportedly includes social security numbers, phone numbers, names, physical addresses, and driver licenses information

Report: Alaska's cellphone emergency alert system malfunctioned during the last earthquake

Experts still working to figure out what went wrong

BEST OF SECURITY TECHNOLOGY EXECUTIVE

Physical Security's #1 Cybersecurity Requirement

By Ray Bernard, PSP, CHS-III

How can you determine what your top cybersecurity concerns are for your electronic security systems?

Mc Cumber Cube Bernard Column

PRODUCT WATCH

AirAccess ACaaS Solution from Alarm Lock

Genetec's SharpV ALPR Cameras

Suprema X-Station 2 intelligent access control terminal

Hy Net(400)

HySecurity HyNet connectivity gate management systems

MEDIA CENTER

SIW8181Webinar300X250

Webinar: How to Approach Corporate Risk From a Management and Oversight Perspective

Be sure to join us on Aug. 18 at 11 a.m. ET as our panel of experts discuss the hot issues impacting corporate risk and its interdependence with security dogma and technology.

Click Here to Register!

EVENT WATCH



Webinar: AI - Video and Beyond

08/31/21 12:00 PM CDT - 08/31/21 1:00 PM CDT
https://event.webcasts.com/starthere.jsp?ei=1486130&tp_key=3b199ed6fa&sti=EW

AI (Artificial Intelligence) is dramatically changing the way users interact with their security systems. Today there are millions of cameras deployed globally generating more recorded video than security operators can possibly keep up with. AI…

Home | Contact Us | Subscribe | Advertise

© 2021 All rights reserved, Endeavor Business Media, LLC.

This email is being sent to david.crouse@pol.state.ma.us.

Please add news.southcommmail.com and mail.southcommmail.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Forward to a Friend | Customer Service Center | Read Privacy Policy

If this email was forwarded to you and you are interested in subscribing, please click here to sign-up.

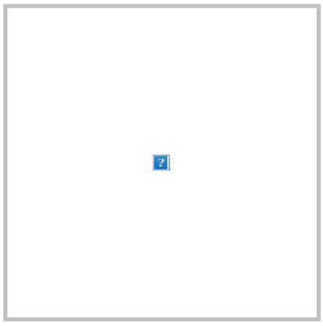
If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Security Info Watch
Endeavor Business Media
331 54th Avenue N.
Nashville, TN 37209

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Sheriff: Tiger Woods was speeding; UOF experts testify in Chauvin trial
Date: Wednesday, April 7, 2021 5:24:45 PM

April 7, 2021 | View as webpage

TOP STORIES



More officers add to tally of police testifying against Chauvin

A UOF expert testified that the ex-officer's knee on Floyd's neck wasn't part of department training

Tiger Woods was speeding before crash, sheriff says

Chicago mayor calls for new foot pursuit policy after fatal OIS

Detroit police chief, others blast 'compassionate release' of suspect in officer's slaying

Turning off AC ends Calif. airport standoff with man in crisis

'Crisis Cops' documentary available for virtual screenings

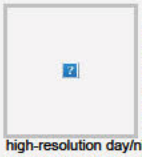
On-Demand Webinar: Using Data To Support Community Policing Strategies



Learn how Stockton PD initiated a new strategy to address firearm crime using data analysis to deploy resources more efficiently, prevent crime and interrupt violence.

Watch now

Precision LIDAR Based Automated Speed Enforcement



The new DragonEye Defender offers fixed-installation automated speed enforcement combining DragonEye's advanced LIDAR technology with high-resolution day/night imaging. Perfect for school zones or high-speed roadway enforcement.

More details

CASE REVIEW



Big case for cops creates conundrum for court

By Val Van Brocklin

And could significantly expand warrantless entries into homes



Welfare check leads to valid frisk and seizure of gun

By Ken Wallentine

The initial contact was in response to the welfare check, and the deputy's actions were reasonably related to community caretaking



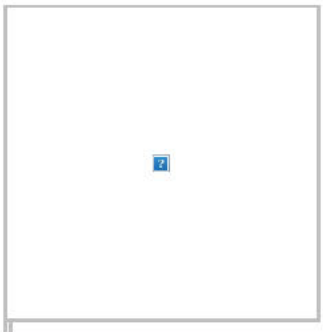
Seventh Circuit reverses a $44 million civil rights verdict against City of Chicago

By Mike Callahan

Court rules that Chicago police officer acted as private citizen when shooting and seriously wounding a friend

Improve Efficiency With Mobile ALPR

Learn how highly advanced mobile ALPR technology with powerful AI software





greatly enhances your department's efficiency and saves on time and resources.

Learn more

ACTIVE SHOOTER RESPONSE



4 things LE should do on social media during an active shooter incident

By Julie Parker

Every police agency should include a social media communications policy in its active shooter response protocols to ensure timely delivery of information



How can we solve the problem of active shooters?

By Lt. Dan Marcou

By aggressively problem-solving this deadly phenomenon, we become part of the solution



LE takeaways from the largest database of life histories of U.S. mass shooters

By Chief Joel F. Shults, Ed.D.

Researchers say being part of a set of available and long-term resources to preempt active shooters is far more important than annual active shooter drills



SPONSORED CONTENT



How police crisis clinicians and LEOs can work together to better serve a community's needs

When social service professionals are properly integrated, they can give departments the expertise to handle mental health incidents while giving community members the help they need.



FEATURED VIDEO



Black Hills Ammunition. The Quest for Perfection.

An inside look at Black Hills Ammunition's quest for perfection.

FEATURED JOB



Now Hiring Lateral and Recruit Police Officers

Top Pay: $105,248 annual

FEATURED COMPANY NEWS

Digital Ally inks new multi-year contract to outfit officers and vehicles with body-worn and in-car camera systems



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Tenn. cop shot in 911 call "setup"; Video: Man rams cruiser, starts firing
Date: Wednesday, May 5, 2021 12:25:35 PM

May 5, 2021 | View as webpage

Dear Police1 Member,

Since distribution of the COVID-19 vaccine began in mid-December, more than 250 million doses have been administered in the United States, with just over a third of the U.S. population fully vaccinated. Have you received a COVID-19 vaccine yet? Click here to answer this week's poll.

Stay safe,

— The Police1 Team

TOP STORIES

Police: Nashville cop shot, wounded by 911 caller's 'setup'

Police say the caller – who had reported an active shooter – opened fire when officers arrived

Video: Okla. man rams patrol car before firing at officer

'ACAB!' motel sign ignites fury, debate in NC tourist town

Video: SRO rescues 'momma duck' and ducklings

Firing of Atlanta officer who shot Rayshard Brooks reversed

Chauvin's lawyer seeks new trial, hearing to impeach verdict

Make the Most of the Space in Your Cockpit

In Mission Critical situations—you're covered. Critical evidence is securely captured from body-worn cameras to in-car video systems and then accessed immediately with our robust digital evidence software.

Contact us for your quotation

Trijicon Credo® 1–6x24 Equips You With Confidence

Law enforcement trusts the Tr jicon Credo® 1-6x24 for its rapid target acquisition made possible by intuitive reticles and extra wide field of view in first or second focal plane options.

Upgrade your riflescope

FEATURED CONTENT



Court ruling helps officers suffering PTSD from a critical incident

By Val Van Brocklin

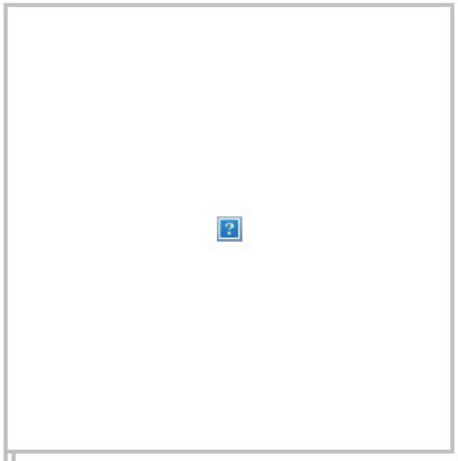
Killing someone is not an "expected, usual, ordinary stress of the job"



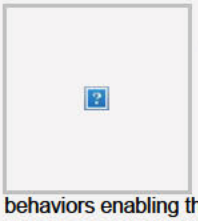
A letter to the American public: How police foundations facilitate positive police-community engagement

By Tom Kovach

A new report highlights many examples of positive community-police engagement from 58 police foundations



Predict Criminal Patterns With ALPR



Learn how powerful ALPR cameras combined with advanced analysis software allow law enforcement to identify and predict suspect behaviors enabling them to effectively pursue and prevent crime.

Find out more

CAREER DEVELOPMENT



Roundtable: How to develop a winning opening statement

By Nancy Perry

Explain with confidence, but

not bravado, that you are the candidate the agency is looking for



Roundtable: Mistakes to avoid during your police promotion oral interview

By Nancy Perry

It is important to set yourself out from your peers as you succinctly articulate a response to each question

FEATURED VIDEO



See the Stun-Cuff in action

The Stun-Cuff is designed to attach directly to a prisoner's leg or wrist and be fired remotely, delivering a five-second burst of fifty thousand volts.

FEATURED DEAL



Use of Force - Expert Guidance for Decisive Force Response 2nd Ed

Buy now!



Police1 does not send unsol cited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Vis t our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: Rizos, Byron (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:37:11 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: Dorian, Christine (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:36:21 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: Lavoie, Marc (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:36:19 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: Upton, Paul (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:36:01 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: McCarthy, Steven (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:04:46 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: Cronin, John E (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:02:18 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: Mcginn, Daniel (POL)
Subject: Top Police Product Picks Inside This Bulletin!
Date: Thursday, August 12, 2021 7:37:21 AM

August 12, 2021 | View as webpage

The Lenco BearCat® G3: Armored Off-Road Vehicle

The BearCat G3 adapts Lenco's proven armor system for a rugged, off-road vehicle, ideal during natural disasters or rural emergencies.

Learn more about BearCat G3

Definitive Answers. Maximum Flexibility

The Thermo Scientific™ 1064Defender™ Raman Analyzer provides reliable lab-proven technology to fit your agency's narcotics identification needs.

Learn more

New Mounting Solutions for Small Devices

The new RAM Top of Dash Mount securely mounts small devices at an optimal viewing height, with no drilling required.

Pre-order today

Getac Rugged Notebooks, Tablets, In-Car Video + BWC

Visit us at booth #1625 to demo the latest rugged mobile, fixed mount, body-worn and in-car computing solutions.

Learn more here

Importance of Ofc. Wellness in Secondary Employment

PowerDetails provides opportunities to earn additional income while protecting officers from exceeding their physical & mental limits while off-duty.

Learn more

Law Enforcement Is a High-Risk Job...

Data and analytics should help make it safer, not add complexity. Learn how TIBCO Integrated Law Enforcement Platform can help.

Download this complimentary ebook

Needing Flexible Pricing Options for ALPR Solutions?

We can help with a pricing strategy through subscription, conventional & hybrid pricing models; legacy upgrade programs; access to grant assistance partners.

Let's connect!

How To Buy Firearms Storage (eBook)

Download this Police1 firearms storage buying guide to learn key steps for product selection, purchasing and implementation.

Download the eBook

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can opt-out here.

If you no longer wish to receive any email messages from Police1, click here to unsubscribe from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Video: Deadly shootout at explosion scene; Mob jumps on cruiser with LEO inside
Date: Tuesday, May 25, 2021 7:00:25 PM

May 25, 2021 | View as webpage

Dear Police1 Member,

Over the past year, officers and their families have faced some of the biggest challenges that have ever confronted law enforcement. Following the terr ble and tragic death of George Floyd, LEOs experienced a backlash of anger, protests, political opposition and defunding that rocked policing to its core. All of this came amid the worst global pandemic in a century, a direct and dire threat to those serving on the front lines, and we still do not know how many of our officers and their family members have been killed by COVID-19.

Being an officer has never been more difficult or demanding and for many who serve, this has resulted in a deprioritizing of personal wellness. However, it has never been more important to keep your heart, mind and body fit. Officer wellness is key to doing all we can to help improve community relations and officer retention and recruitment as we look toward the future.

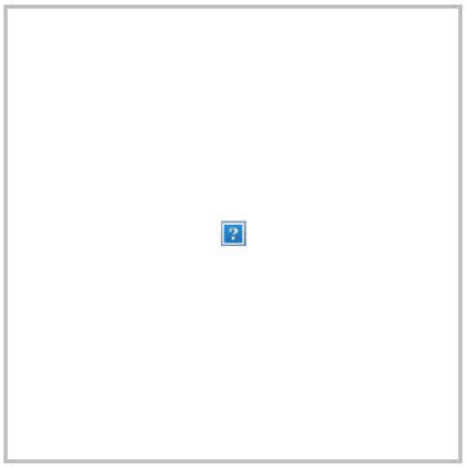
Society outsources the most difficult challenges to law enforcement, and it's only fair that officers have high-quality support when facing their own challenges. Take good care of yourself and your fellow officers. Surround yourself with good people who support you. Talk with peer support. Connect with a high-quality, culturally competent therapist. Do your part to help smash the stigma that makes it so difficult for so many in the profession to seek help.

We thank you for your service, your sacrifices and all you have done to keep our communities safe during the past year.

Stay safe,

— Dr. David Black, founder and CEO of Cordico

TOP STORIES



Video: Triple murder suspect killed in shootout at scene of explosion

The suspect began shooting as soon as the officer stepped out of his vehicle

Video: Mob jumps on cruiser with St. Louis officer inside

Police capture man wanted in 4 killings after week on run

Texas constable's office accused of abusing female deputies

Minn. conservation officer killed in crash on duty

Texas governor vows to sign bill that would make it harder to defund police

Predict Criminal Patterns With

Make End-of-Fiscal-Year Dollars

ALPR

Learn how powerful ALPR cameras combined with advanced analysis software allow law enforcement to identify and predict suspect behaviors enabling them to effectively pursue and prevent crime.

Find out more

Go Further!

Silynx is including a smartphone cable with every Clarus system through June 30. $195 value + free shipping! And save 25% off Eagle and HSI headsets. Offers can be combined! Contact info@silynxcom.com

Maximize your department dollars

FEATURED CONTENT

Policing and civil unrest: 5 changes in law enforcement since 2020

By Police1 Staff

A look at some of the reforms police agencies and cities have implemented

Roundtable: Perspectives on policing one year after the death of George Floyd

By Police1 Staff

Police1 columnists reflect on their analysis of 2020's civil unrest and calls for police reform and share their thoughts on where policing is now

The fallout from the 'defund' movement

By James Dudley

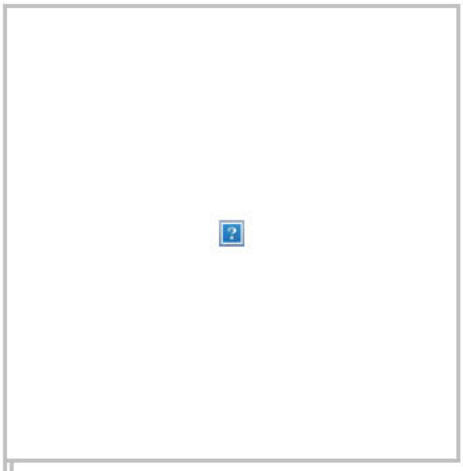
As many experts predicted, we have seen a rise in violent crime accompanied by an increase in officer retirements and resignations

One Mans' Quest to Prove His Innocence



Join Bensalem Township Director of Public Safety Fred Harran and exoneree James Tillman as they discuss the wrongful conviction that sent James to prison for over 18 years.

Register now



PERSONAL PERSPECTIVES



Opinion: Why getting offline could help us return to truth and unity

By Booker Hodges

Sylvester McMonkey McBean is controlling our thoughts, and, at some point, we have to stop feeding him our time and energy



Opinion: Do we still have consent?

By Haywood Irving

There is a perception that politicians and LE leaders are making public safety and personnel decisions based on what the loudest voices demand



SPONSORED CONTENT



The ABCs of narcotics field testing

3 testing techniques in

these advanced drug detection kits improve accuracy and sample integrity as well as keep officers safer from exposure.

FEATURED VIDEO



The Power of Performance

Black Hills Ammunition's new 300 Blackout 115 grain Dual Performance round

FEATURED PRESS RELEASE



How To Buy Online Training Systems

Download the guide

Pol ce1 does not send unsolicited messages. You are receiving this email because you have signed up for Pol ce1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Video: Man fires cop's holstered gun; Slain Ind. detective was ambushed
Date: Thursday, July 8, 2021 3:33:10 PM

July 8, 2021 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES

Video: Man shoots Las Vegas officer with officer's holstered gun

The department is now reviewing if it needs to stop using that style of holster

Ind. detective killed outside federal office was ambushed, FBI says

$1B in illegal pot seized in largest Los Angeles County bust

Video: Officer finishes DoorDash delivery after company driver is arrested

Video: Fleeing suspect spins around and pulls gun on officer, is killed

California shifts police shooting probes to attorney general

2-3.PNG?w=300&format=jpg&quality=87

Why You Should Ditch Your Clunky 'Throw' Phones

Read how Sacramento crisis negotiators ditched heir clunky 'throw' phones, and why you should, too in this exclusive ar icle.

Read the article

FEATURED CONTENT

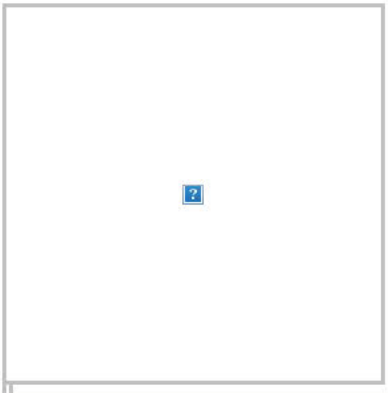
Opinion: Change that is good for police and community members

By Currie Myers

Whatever term you use to describe he changes needed in policing, the goal is to improve it in ways that will benefit both communi ies and law enforcement

No PIO? How small police departments mitigate communication challenges without a dedicated public information

officer
By Evan Bloom
Implementing effective stakeholder communica ions is achievable by using the relevant resources and he correct planning



Pursue and Prevent Crime With ALPR



Jenop ik's powerful ALPR and data analysis enable you to monitor suspect vehicles and evaluate data in real time, securely and accurately to combat crime.

Learn more

GUN RETENTION



Video: Coaching gun retention from a cross grab technique

By Jerrod Hardy

Retaining a firearm is of critical importance for an officer; here's how to secure your firearm when a subject reaches with a cross grab



Training day: Gun retention techniques

By Lindsey J. Bertomen

Gun retention training is essential to help cops survive poten ially fatal attacks – incorporate these eight techniques into your police firearms training



SPONSORED CONTENT



Training in a post-pandemic world

In this report, we identify five ways agencies use online learning to achieve training goals, maximize their training budgets and increase the effectiveness of their in-person training.

FEATURED JOB

Now Hiring Lateral and Recruit Police Officers

Top Pay: $105,248 annual

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive

$6,118-$7,807* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you are a Police1 member and subscribed to this newsletter.

If you do not want to receive this newsletter, you can **opt-out here.**

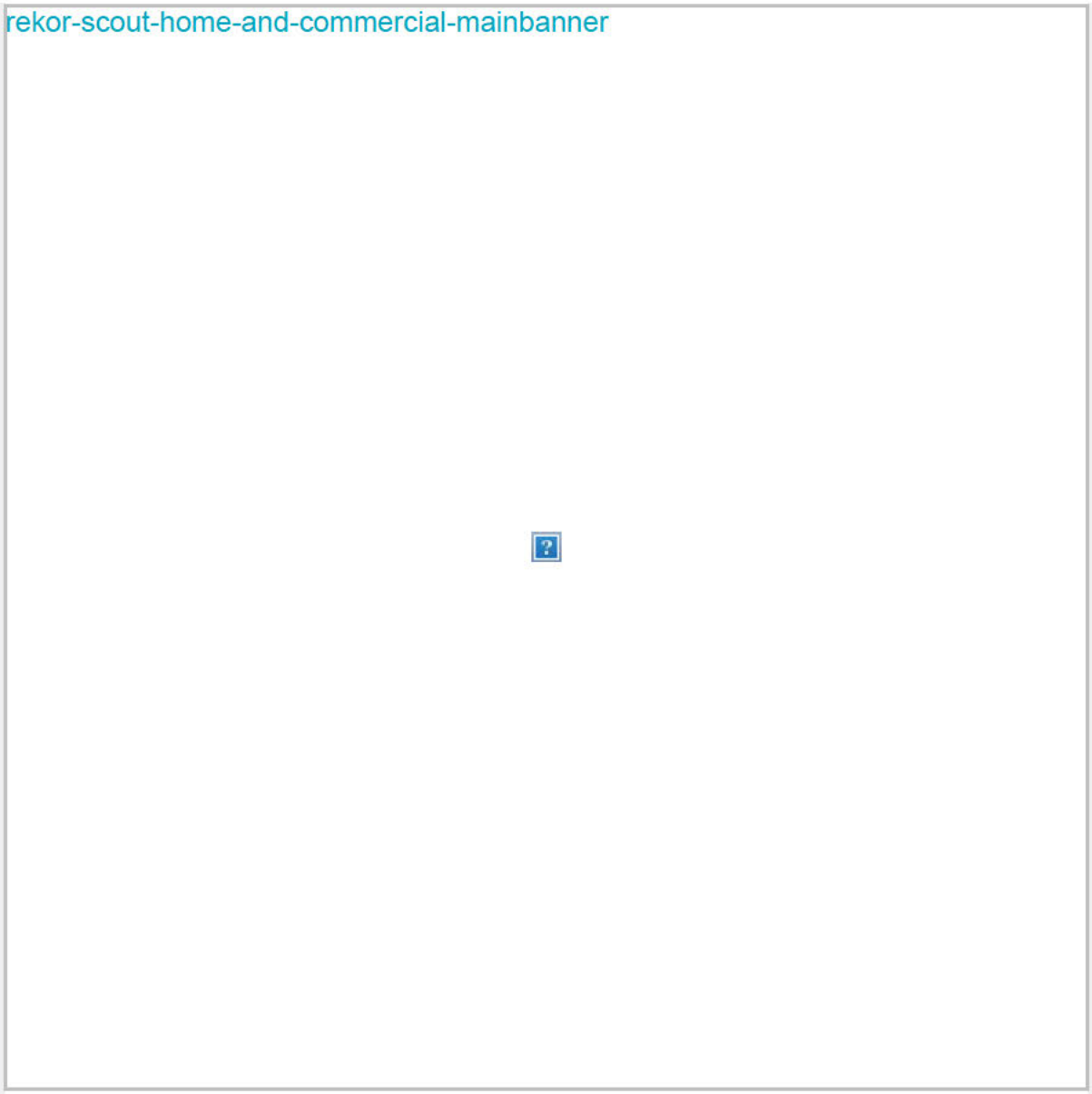
If you no longer wish to receive any email messages from Police1, **click here to unsubscribe** from all mailings.

Copyright © 2021 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Rekor Systems, Inc.
To: Ferguson, Gary E (POL)
Subject: Watchman is now Rekor Scout™
Date: Wednesday, January 13, 2021 11:08:49 AM

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

Rekor-Banner-Horizontal-Color-Tag



We are excited to announce that Watchman is now Rekor Scout™!

Scout brings you all of the features you know and love with customizable hot list alerts, easy connection to most IP enabled cameras, and AI-powered vehicle and license plate recognition.

Our Scout update launching January 13, 2021 at 8pm ET packs new features that benefit commercial and home users.

New Rekor Scout™ Features

Advanced User Management*: Simplifies the User Account Creation and Management with the creation of Groups with definable privileges such as specific Hot Lists and Camera sets for alerting and searching.

Data Sharing and Control: Rekor redefines the sharing paradigm within the ALPR market space with completely open and secure sharing capability enabling:

- **Federated Peer-to-Peer Secure Searching:** Privacy and control is at the center of federated search which is an infrastructure option that allows companies to define who may search their data via defined and secure search pathways.
- **3rd Party Sharing through API:** ALPR content is owned by the collecting agency and as such, Rekor makes a series of API's available to allow for the transfer of content out of Rekor solutions and into 3rd party databases or vice versa.

Customizable Data Retention*: Establish custom data retention policies for "Hits", "Hit & Types" vs. passive reads. This gives complete control over retention policy to the company.

**not available for Rekor Scout™ Home subscribers.*

View Rekor Scout

Start free trial

rekorgo-pencil-banner



Rekor Systems, Inc., 7172 Columbia Gateway Drive, Suite 400, Columbia, MD 21046, (410) 762-0800
Unsubscribe Manage preferences

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: WEBINAR: Addressing Ethics and Privacy in Police Technology
Date: Thursday, July 29, 2021 9:09:34 AM

AxonWebinar8.10.2021.jpg

Technology is evolving at a faster rate than ever. Simultaneously, public concern over government surveillance and intrusions on privacy rights are also growing. Axon (Formerly TASER International) has successfully introduced some of the most impactful – and controversial public safety technologies of the past 25 years including TASER weapons, body cameras, cloud software, and artificial intelligence based software services including automated license plate recognition (ALPR).

Join Rick Smith, CEO, Director, and Founder Axon (Formerly TASER International) and Regina Holloway, Vice President of Community Impact at Axon, who will share insights and lessons learned in navigating issues related

to public perceptions, ethics and privacy protections, and community engagement as critical elements in introducing new public safety technologies.

Register Now!

Presenters

Rick_Smith.jpeg

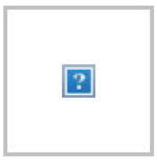
Rick Smith
Founder & CEO, Axon Enterprise

Rick Smith has served as Chief Executive Officer and as a director of the Company since 1993. He is a co-founder of the Company. After graduating from Harvard Cum Laude in just three years (class of 1991), Mr. Smith entered directly into the Masters of Business Administration Program at the University of Chicago, the youngest person accepted into his class at the business school. In two years, he completed both his M.B.A. with honors at the University of Chicago (normally a two-year program in itself) graduating in the top 5% of his class and a Masters Degree in International Finance from the University of Leuven in Leuven, Belgium. After graduating from graduate school in the summer of 1993, he immediately co-founded TASER International with his brother on September 7th of 1993. The company changed its name to Axon in April 2017 when the revenue bookings for their cloud software and wearable sensors business unit surpassed the scale of the original TASER weapons segment.

Regina Holloway
VP Community Relations, Axon Enterprise

Regina Holloway is the VP of Community Impact at Axon. Previously Regina was a Sr. Program Manager at the Policing Project at NYU School of Law, where she helped to implement the Neighborhood Policing Initiative in the City of Chicago. Before joining the Policing Project, Regina served as a Supervising Investigator with the Civilian Office of Police Accountability in Chicago. There, she supervised a

Major Case Squad which investigated officer-involved shootings. She began her legal career as a Clinical Fellow at Suffolk University Law School, where she developed housing discrimination investigations. That work led to the publication of a study on housing discrimination experienced by trans and gender non-conforming residents in the Boston area. The study was published in Yale Law School's Journal of Law and Feminism. Thereafter, Regina practiced criminal defense in the Boston District Courts, where she worked as a Bar Advocate for Suffolk Lawyers for Justice. Regina is a Senior Atlantic Fellow for Racial Equity through a partnership between Columbia University and the Nelson Mandela Foundation. She holds a Bachelor of Arts in Political Science and African-American Studies from Temple University and earned her Doctor of Jurisprudence from Suffolk University Law School.





LEARN MORE

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

UNSUBSCRIBING from this email will STOP ALL EMAILS from the FBINAA

You can edit your Communication Preferences from your Profile on the FBINAA Website.

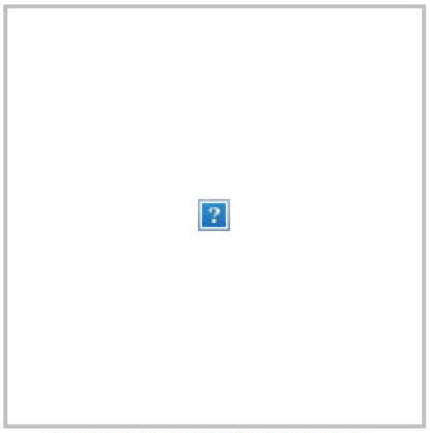
Share This Email | Share This Email | Share This Email | Share This Email

FBI National Academy Associates, Inc. | FBI Academy, Building 8-102, Quantico, VA 22135

Unsubscribe steven.mccarthy@pol.state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with



Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: WEBINAR: Addressing Ethics and Privacy in Police Technology
Date: Thursday, August 5, 2021 9:09:36 AM

AxonWebinar8.10.2021.jpg

Technology is evolving at a faster rate than ever. Simultaneously, public concern over government surveillance and intrusions on privacy rights are also growing. Axon (Formerly TASER International) has successfully introduced some of the most impactful – and controversial public safety technologies of the past 25 years including TASER weapons, body cameras, cloud software, and artificial intelligence based software services including automated license plate recognition (ALPR).

Join Rick Smith, CEO, Director, and Founder Axon (Formerly TASER International) and Regina Holloway, Vice President of Community Impact at Axon, who will share insights and lessons learned in navigating issues related

to public perceptions, ethics and privacy protections, and community engagement as critical elements in introducing new public safety technologies.

Register Now!

Presenters

Rick_Smith.jpeg

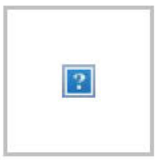
Rick Smith
Founder & CEO, Axon Enterprise

Rick Smith has served as Chief Executive Officer and as a director of the Company since 1993. He is a co-founder of the Company. After graduating from Harvard Cum Laude in just three years (class of 1991), Mr. Smith entered directly into the Masters of Business Administration Program at the University of Chicago, the youngest person accepted into his class at the business school. In two years, he completed both his M.B.A. with honors at the University of Chicago (normally a two-year program in itself) graduating in the top 5% of his class and a Masters Degree in International Finance from the University of Leuven in Leuven, Belgium. After graduating from graduate school in the summer of 1993, he immediately co-founded TASER International with his brother on September 7th of 1993. The company changed its name to Axon in April 2017 when the revenue bookings for their cloud software and wearable sensors business unit surpassed the scale of the original TASER weapons segment.

Regina Holloway
VP Community Relations, Axon Enterprise

Regina Holloway is the VP of Community Impact at Axon. Previously Regina was a Sr. Program Manager at the Policing Project at NYU School of Law, where she helped to implement the Neighborhood Policing Initiative in the City of Chicago. Before joining the Policing Project, Regina served as a Supervising Investigator with the Civilian Office of Police Accountability in Chicago. There, she supervised a

Major Case Squad which investigated officer-involved shootings. She began her legal career as a Clinical Fellow at Suffolk University Law School, where she developed housing discrimination investigations. That work led to the publication of a study on housing discrimination experienced by trans and gender non-conforming residents in the Boston area. The study was published in Yale Law School's Journal of Law and Feminism. Thereafter, Regina practiced criminal defense in the Boston District Courts, where she worked as a Bar Advocate for Suffolk Lawyers for Justice. Regina is a Senior Atlantic Fellow for Racial Equity through a partnership between Columbia University and the Nelson Mandela Foundation. She holds a Bachelor of Arts in Political Science and African-American Studies from Temple University and earned her Doctor of Jurisprudence from Suffolk University Law School.





LEARN MORE

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

UNSUBSCRIBING from this email will STOP ALL EMAILS from the FBINAA

You can edit your Communication Preferences from your Profile on the FBINAA Website.

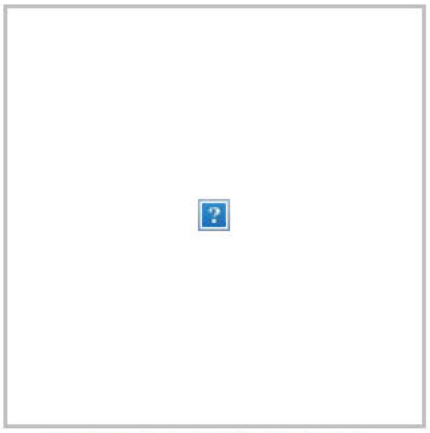
Share This Email | Share This Email | Share This Email | Share This Email

FBI National Academy Associates, Inc. | FBI Academy, Building 8-102, Quantico, VA 22135

Unsubscribe steven.mccarthy@pol.state.ma.us

About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with



Try email marketing for free today!

From: Maureen Mulvaney
To: Egnitz, Brian (POL)
Subject: What you missed
Date: Wednesday, November 17, 2021 5:07:32 PM

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

Brian,

Yesterday over 100 law enforcement agencies across the country joined us for our educational webinar "Combating Gun Violence with Technology." We were joined by Amazon Web Services (AWS) justice and public safety team and Captain Jason Potts from Vallejo Police Department.

During the webinar we discussed:

- Influencing policy around "ghost guns"
- How to rally your community around gun violence and "sideshow" prevention, including Vallejo PD's four part-plan for crime reduction and community policing
- How to leverage technology and data, such as pairing detection and ALPRs, to improve clearance rates and drive down violent crime rates

You can view the webinar here, as well as gain access to a playbook and additional resources around how audio detection and ALPR evidence capture can unlock investigative leads to reduce gun violence in your area.

Maureen Mulvaney
Director, Product Marketing

Unsubscribe from email communications

Flock Safety
1170 Howell Mill Rd NW ,
UNIT 210
Atlanta, GA 30318

From: Maureen Mulvaney
To: Mason, Christopher (POL)
Subject: What you missed
Date: Wednesday, November 17, 2021 5:07:31 PM

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

Christopher,

Yesterday over 100 law enforcement agencies across the country joined us for our educational webinar "Combating Gun Violence with Technology." We were joined by Amazon Web Services (AWS) justice and public safety team and Captain Jason Potts from Vallejo Police Department.

During the webinar we discussed:

- Influencing policy around "ghost guns"
- How to rally your community around gun violence and "sideshow" prevention, including Vallejo PD's four part-plan for crime reduction and community policing
- How to leverage technology and data, such as pairing detection and ALPRs, to improve clearance rates and drive down violent crime rates

You can view the webinar here, as well as gain access to a playbook and additional resources around how audio detection and ALPR evidence capture can unlock investigative leads to reduce gun violence in your area.

Maureen Mulvaney
Director, Product Marketing



Unsubscribe from email communications

Flock Safety
1170 Howell Mill Rd NW ,
UNIT 210
Atlanta, GA 30318



From: Maureen Mulvaney
To: Clement, Michael (POL)
Subject: What you missed
Date: Wednesday, November 17, 2021 5:07:34 PM

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

Michael,

Yesterday over 100 law enforcement agencies across the country joined us for our educational webinar "Combating Gun Violence with Technology." We were joined by Amazon Web Services (AWS) justice and public safety team and Captain Jason Potts from Vallejo Police Department.

During the webinar we discussed:

- Influencing policy around "ghost guns"
- How to rally your community around gun violence and "sideshow" prevention, including Vallejo PD's four part-plan for crime reduction and community policing
- How to leverage technology and data, such as pairing detection and ALPRs, to improve clearance rates and drive down violent crime rates

You can view the webinar here, as well as gain access to a playbook and additional resources around how audio detection and ALPR evidence capture can unlock investigative leads to reduce gun violence in your area.

Maureen Mulvaney
Director, Product Marketing



Unsubscribe from email communications

Flock Safety
1170 Howell Mill Rd NW ,
UNIT 210
Atlanta, GA 30318



From: Rekor Systems, Inc.
To: Plante, Michelle (POL)
Subject: Meet Rekor Blue™ – ALPR App For Law Enforcement
Date: Tuesday, November 23, 2021 10:29:21 AM

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

rekor_intelligence-driven-innovation

Rekor Blue Overview — Video



Meet Rekor Blue™

A powerful new tool to support scene investigations

Rekor Blue is the first ALPR smartphone app designed specifically for law enforcement. Built using the same AI recognition engine as Rekor Scout™, Blue delivers advanced data capture in the palm of the hand. Officers now have access to extremely accurate license plate recognition, whenever and wherever.

RekorBlue-map

Rekor Blue™ Benefits

- Portable for on-the-go and discreet applications
- Secure Rekor Scout™ integration
- Alerts from connected CJIS, NCIC, and department hotlists
- Search and review reads instantly
- Works without cellular or Wi-Fi

Rekor Blue™ Spec Sheet

Learn more about Rekor Blue™

Special Offer

Take advantage of Rekor Blue for FREE!

Download the app and complete the Agency Verification process to connect to your current Scout environment. Then have your officers download the app to begin scanning plates and receiving alerts on their phone.

This gives **all officers** in your department **unlimited* access to Blue** through the end of 2021, **FREE!**

*Unlimited scans, once the agency is verified and the user is approved by the department administrator.
*Extended trial period provides free access through December 31, 2021. After this extended trial period app access will be $24.99 per month or $249.99 per year per device.

Get Started Today:

1. Download the Blue app
2. Register new account
3. Verify your agency

apple-app-store-badge



google-play-badge



Want to learn more or have questions? **Let us know**.

The Rekor Team
E sales@rekor.ai
P (410) 762-0800



Rekor Systems, Inc., 6721 Columbia Gateway Drive, Suite 400, Columbia, MD 21046, (410) 762-0800
Unsubscribe Manage preferences

AAMVA

American Association of
Motor Vehicle Administrators

technology
POLICY security
Safety training
REVENUE Data
ACCURACY



License Plate Reader Program
Best Practices Guide





October 2021

LAW ENFORCEMENT STANDING COMMITTEE
VEHICLE STANDING COMMITTEE

2021 © Copyright All Rights Reserved
American Association of Motor Vehicle Administrators

Cover photo credits: © iStockphoto.com

Contents

Executive Summary 2

Chapter 1 Introduction 3

Chapter 2 License Plate History 5

Chapter 3 License Plate Reader Fundamentals 9

Chapter 4 License Plate Reader Benefits 17

Chapter 5 License Plate Readers as a Tool to Improve Toll, Commercial Motor Vehicle, and Border Operations 20

Chapter 6 License Plate Reader Program Best Practices for Law Enforcement 24

Chapter 7 License Plate Reader Success Stories 28

Appendix A Significant License Plate Reader Court Cases and Applicable Federal Statutes 30

Appendix B Additional License Plate Reader Resources 34

Appendix C Sample License Plate Reader Policies 35

Appendix D AAMVA License Plate Reader Working Group Roster 49

Executive Summary

Since their inception more than a century ago, license plates have primarily been used to display information for fast and accurate identification of motor vehicles and to demonstrate compliance with motor vehicle registration laws.

In support of their highway and public safety missions, License Plate Readers (LPRs) provide law enforcement with the ability to check license plates against various databases. Tolling and parking enforcement authorities also rely on LPR technology for the collection of tolls and enforcing parking regulations.

Law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety.

More than a decade ago, it was recognized that inconsistent business rules used by license plate issuing authorities were resulting in alarmingly high "misreads," diminishing law enforcement's ability to identify and apprehend suspected criminals and terrorists, recover stolen vehicles, and assist people in need of assistance. Similarly, tolling and parking authorities are hampered in their revenue collection mandates that are critical to maintaining infrastructure and ensuring parking regulations are not flouted. In addition, license plate misreads hamper Customs and Border Protection's ability to correctly identify vehicles crossing international borders.

In response to this issue, in 2012, AAMVA published a *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design & Manufacture*. At the time, AAMVA did not have a License Plate Standard. Since that time, AAMVA has published a License Plate Standard (2016) and a License Plate Standard, Edition 2 (2020).

In 2020, the AAMVA Law Enforcement and Vehicle Standing Committees determined the 2012 LPR document should be retained but with content now covered in the License Plate Standard removed and the remaining material updated and added to as appropriate. This guide has been renamed *License Plate Reader Program Best Practices Guide* and has been refocused on best practices in the administration of LPR Programs for state and provincial law enforcement, although much of the content is applicable to tolling and parking enforcement authorities alike.

Chapter 1 Introduction

License Plate Readers (LPRs) are an effective law enforcement and traffic safety tool and are critical to government entities—such as tolling and parking enforcement authorities—who use the technology to enforce the law and collect revenue. LPRs enhance public safety and security by providing law enforcement the ability to check license plates against databases such as the National Crime Information Center. The databases searched are at the discretion of each law enforcement agency using LPR technology.

Federal, state, local, and tribal public safety agencies rely on accurate and timely license plate information to effectively and efficiently perform the multiple tasks required in the performance of their duties. Information is available in multiple formats, including hot lists (e.g., stolen vehicle), Be On the Look Out (BOLO), Attempt to Locate (ATL), officer safety information, AMBER Alerts for at-risk children, SILVER Alerts for at-risk adults, and more. Much of this information can be, and often is, associated with a vehicle's license plate. The ability of LPRs to quickly and accurately scan thousands of license plates is critical to the men and women of law enforcement who contact hundreds of thousands of people throughout the U.S. and Canada every day, as well as to Customs and Border Protection officers and agents monitoring international ports of entry. When LPRs misread license plates, law enforcement is hampered in its mission to protect and to serve, and government entities lose revenue from uncollected tolls.

The International Association of Chiefs of Police conducted a 2021 survey of police agencies across the U.S. about their use of LPR systems. More than 1,200 agencies responded to the survey measuring LPR use, policy considerations, data retention and management, and more.[1]

Among all respondents:

- **40%** reported currently using LPR systems in their departments.
- Cost was the biggest barrier to LPR use.
- Larger agencies were more likely to use LPR systems than smaller agencies were.
- Mobile units were the most common form of LPR system used.

Among agencies using LPR:

- **75%** owned their own LPR system. Others contracted use of their LPR system or leveraged another agency's LPR system.
- **63%** shared their system with another agency, and **84%** shared their LPR data with other agencies.
- **64%** reported full control of the data in their LPR system.
- **44%** of the agencies using LPR stored their data on the cloud, and **43%** stored their data on agency servers or other government resources.

A study conducted by the Police Executive Research Forum[2] concluded that LPRs increased license plate reads by a factor of more than eight. What the study did not, and could not reveal, is the number of hits "missed" because of license plate misreads. Regardless of the misread rate in a particular jurisdiction, there

1 As of this printing, these represent preliminary estimates only.

2 Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology: Police Executive Research Forum, December 2011.

is no refuting that misreads occur. And when they do, the potential exists to miss opportunities to arrest a suspected criminal or terrorist, to recover a stolen vehicle, or to collect toll revenue.

A completely effective "ecosystem" is needed to ensure as close to 100% as possible accurate license plate read rate is achieved by LPRs. Multiple stakeholders share the responsibility for maintenance of the ecosystem. Motor vehicle agencies having license plate design and manufacture administration oversight responsibility should ensure their issued license plates align with the AAMVA License Plate Standard (see Appendix B). LPR manufacturers have a responsibility to develop and implement state of the art technology to accurately read the multi-variant license plates that exist. Law enforcement and other government entities using LPR are responsible for ensuring they have policies and training that align with the most current best practices available.

AAMVA published a *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design & Manufacture*. At the time, AAMVA did not have a License Plate Standard. Since that time, AAMVA has published a License Plate Standard (2016) and a License Plate Standard, Edition 2 (2020) (see Appendix B).

This LPR Program Best Practices document, combined with the AAMVA License Plate Standard, Edition 2; License Plate Policy Statements; and License Plate Verification Program all serve to assist jurisdictions in shaping of jurisdiction laws and regulations and operational policies ensuring license plate readability and integrity.

In 2020, the AAMVA Law Enforcement and Vehicle Standing Committees determined the 2012 document should be retained but with content now covered in the License Plate Standard removed and the remaining material updated and added to as appropriate. This guide has been renamed *License Plate Reader Program Best Practices Guide* and has been refocused on best practices in the administration of LPR Programs for state and provincial law enforcement, although much of the content is applicable to tolling parking enforcement authorities alike.

AAMVA also has four policy statements addressing license plates (see Appendix B).

In 2020, AAMVA launched the License Plate Verification Program (LPVP). The LPVP allows jurisdictions to submit up to four license plates per fiscal year for examination and comparison with the AAMVA License Plate Standard, at no cost to the jurisdiction. The examination is conducted by an independent third-party laboratory under contract with AAMVA. A written report is provided to the submitting jurisdiction outlining areas where their license plate(s) do, and do not, align with the License Plate Standard. The report identifies for jurisdictions areas for potential improvement in the readability of their license plates.

Chapter 2 License Plate History

Introduction

Since their inception more than a century ago, license plates have primarily been used to display information for fast and accurate identification of motor vehicles and to demonstrate compliance with motor vehicle registration laws. The advancement of manufacturing technology has resulted in more colorful and detailed graphics on plates, which can be used to promote a jurisdiction or organization but at times have created an identification challenge for law enforcement and a readability challenge for camera technology. Most jurisdictions now have numerous plate types and designs available to the public.

Hand-Made, Horse-Drawn

The first record of a registration plate in the U.S. was in Philadelphia, Pennsylvania, in the 1850s. Even then, legibility of plates was a concern, and horse-drawn vehicles required registration to be identified with numbers "not less than four inches high." Among other things, these numbers provided a means of identification when reporting an incident involving inappropriate or reckless driving. Today, only the state of Indiana still requires a license plate on a horse-drawn carriage.

The construction of these early registration plates was left to the innovation of the vehicle owner; wood, brass, or other metals affixed to leather backings were common materials used. During the next 50 years, many cities required registration, and they frequently required payment of a modest registration fee.

Plate Production and Issuance

In the early 1900s with the advent of motorized vehicles, jurisdictions took responsibility for registration and standardization of plate issuance.

In 1901, New York became the first state to require license numbers on motor vehicles. In 1903, Massachusetts was the first state to issue a standard statewide plate. Others soon followed, but issuance of plates remained inconsistent.

California also began requiring plates in 1903 but did not produce them; the Automobile Club of Southern California (an early AAA organization) issued license plates—called mouse ears—to members for $1.00. The state assumed this responsibility in 1910.

On March 22, 1905, the Maine senate debated House Document 552, which required automobiles to be registered and plates to be issued. A senator argued in favor of the plate by stating: "The point upon this bill comes is upon the matter of registration. What does it mean? The matter of registration does not prevent the violation of the law, but the matter of registration, and the law compelling the carrying in a conspicuous position, of a certain number, which leads to the registration and which may lead to the detection or recognition of a violation of the law, is all that registration can amount to as to guarding the safety of the public against accidents from automobiles."

As the debate continued, another senator voiced his support for the display of a number on automobiles so that the operator could be identified when it frightened a horse. In part he stated, "I do not own

an automobile, and do not ever expect to. I do own a cheap horse and have a wife and three girls that drive it. What is the result now? They do not dare to go out. I have a safe horse, but when one of those reckless fellows comes along (*in an automobile*), they are likely to get tipped out, as many have in the State of Maine."

The debate continued, the bill passed and became public law Chapter 147. It required the Secretary of State to license operators, to register automobiles and motorcycles, and to issue plates. The law also required the Secretary of State to "furnish the applicant two enameled iron plates containing the word 'Maine' and the number of the registration in Arabic numerals not less than four inches in height. The number plates must be attached to the front and back of the automobile and one number plate must be attached to the back of motorcycles."



Maine plate, 1905 to 1911. The width changed based on the number of characters on the plate.



Starting in 1903, "mouse ear" plates were sold for $1 by the Automobile Club of Southern California.

By 1915, nearly all jurisdictions issued license plates on an annual basis and charged a registration fee that allowed a vehicle to be driven on public roads. Government officials recognized early on that a registration system provided for vehicle identification and a source of transportation revenue. However, license plate design continued down an inconsistent path. It wasn't until 1956 that a standard plate size (12" x 6") was introduced at the request of automobile manufacturers to make it easier to incorporate license plates.

Integrating Safety Concepts

With the rapid increase in the motor vehicle population in the 1920s and 1930s, traffic crashes increased dramatically, leading to the need to improve not only vehicle identification but also vehicle safety. License plates became one means to improve safety by providing a device that improved the night visibility of motor vehicles. The first retro-reflective license plates in the U.S. were issued by New Mexico in 1936.

As retro-reflective technology advanced, fully retro-reflective plates became possible and the first was issued by Connecticut in 1947 followed by Maine in 1949. Delaware followed suit in 1950 followed by Rhode Island and Oregon in 1951.

During the 1950s, relatively new sheeting gave retro-reflective plates their biggest boost. Minnesota had the distinction of being the first state to use the sheeting on automobile license plates.

The effect that retro-reflective plates had on nighttime motor vehicle crashes was dramatic, and it did not go unnoticed. In 1956, the first year of use in Minnesota, deaths caused by automobile crashes in rural areas dropped from 24% to 9%. Urban area fatalities involving parked vehicles decreased from 28% to 7%.

Standards Materialize

Tiny San Marino—the smallest republic in Europe, with an area of only 24 square miles—had the distinction of being the first country on that continent to make reflective license plates mandatory on all 2,500 of its automobiles. In the other hemisphere, the South and Central American countries of Peru and Costa Rica also became pioneers in retro-reflective license plates. In Canada, the provinces of Newfoundland and Alberta led the way. Today, all 50 U.S. states and most other countries in the world use retro-reflective plates.

With the advent of retro-reflective license plates, law enforcement realized a benefit in improved legibility.

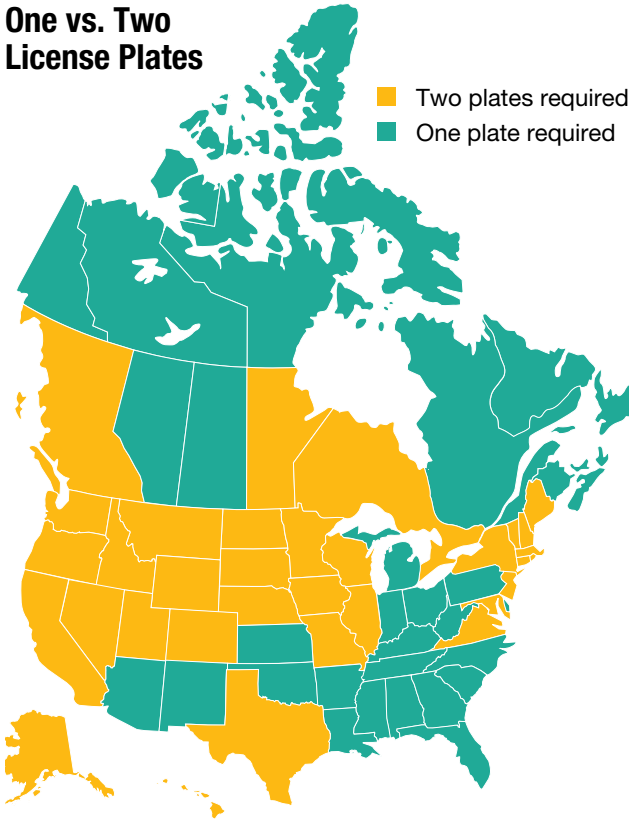
Although one of the original intents of a vehicle registration number was to aid law enforcement, the reality was that non-reflective plates could only be easily read during daylight hours. Retro-reflection provided greatly improved legibility at night, and even today fully retro-reflective plates continue to have strong endorsement from U.S. law enforcement officials, who advocate fully retro-reflective plates on both the front and rear of vehicles for improved safety and law enforcement efficiency.

Although early license plates were often homemade or devised of porcelain, steel became the predominant base material for plates during the first half of the 20th century. Today, aluminum dominates as the material used in license plate manufacture.

After 1945, most states returned to the pre-war practice of requiring two plates per vehicle. Since then some states have moved from two plates to one or vice versa. States typically move to one plate with the intent to save on the cost of the second plate. During the late 1980s, Connecticut was the last state to move from one plate to two plates. Law enforcement effectiveness was cited as the primary reason for the change. The U.S. and Canada are two of a small number of countries that allow one plate. The following chart identifies the North American jurisdictions that require either one or two license plates.

Within the U.S. and Canada, each jurisdiction is responsible for issuing license plates for vehicles registered in their jurisdiction. To create a plate unique and easily recognizable to that jurisdiction, combinations of colors were originally used. Plate background color and colors of the alphanumeric were varied, along with the characters, to create the necessary combinations needed for vehicle classifications and to differentiate plates among the jurisdictions. With increases in vehicle populations and registration classifications, color alone was not enough. Graphic technology became available in the early 1970s that allowed another level of differentiation of license plates. In 1973, Illinois was the first state to use graphics preprinted on the reflective sheeting, for a special plate for disabled veterans. South Dakota quickly followed with the first general issue graphic of Mount Rushmore National Monument. Today all jurisdictions use graphic plate design. When first introduced, graphic design plates were viewed as attractive and as a mechanism to enhance the image of the jurisdiction.

One vs. Two License Plates



Three Canadian jurisdictions require two plates and 10 require one plate. Thirty U.S. States and the District of Columbia require two plates and 20 states require one plate. NOTE: The five U.S. Territories are not included.

However, since the proliferation of graphic plate designs, law enforcement is no longer able to easily recognize the issuing jurisdiction. The widespread use of graphics and colors frequently makes legibility of the plate characters a challenge for law enforcement.

Modern Features, Security, and Function

Until the 1990s, all the U.S. and Canada and most of the rest of the world produced license plates with raised (embossed) alphanumeric characters. In the late

1990s, digital printing technology was introduced, resulting in flat, digitally printed license plates. Today, many states are issuing flat plates. Some jurisdictions issue a combination of embossed and flat plates.

As a result of increasing concern with the use of counterfeit license plates used to perpetrate crimes, security features were added to license plate. These security features allow for easy recognition of fraudulent plates and provides one more obstacle for criminals to overcome.

The following functions of a license plate have been, and continue to be, the most important over the past century:

- Display of information necessary for fast and accurate identification of a motor vehicle and compliance with motor vehicle registration laws
- A validation sticker is issued in most jurisdictions, often rotating the color, to indicate a current and valid registration
- Provide an added margin of visibility and safety by making vehicles more visible

More recently, additional functions of license plates have emerged to

- Provide revenue for highway funds and sponsoring organizations (specialty and vanity plates)
- Use images of plates to improve and increase toll collection, parking fees, and fines
- Provide a way for individuals to express their pride or to promote various causes
- Provide access control to parking, facilities, and gated communities.

Alternative Vehicle License Plates

Two nontraditional license plate technologies have recently emerged: digital license plates and front license plate wraps. These alternative vehicle license plates are intended to replace traditional aluminum or metal license plates.

Digital license plates are reflective but not retro-reflective, creating challenges for law enforcement, tolling authorities, and others that read license plates in all light conditions and rely on License Plate Reader (LPR) technology, which is currently programmed to read retro-reflective license plates.

A license plate wrap is an adhesive license plate applied to a vehicle's bumper. Wraps, where currently authorized for purchase, are only allowed to be applied to the front of a vehicle.

A curved, indented, or otherwise non-flat surface could render the wrap unreadable to LPRs or the human eye.

For a fuller explanation of both the benefits and challenges associated with nontraditional license plates, see the AAMVA License Plate Standard, Edition Two, Chapter 5 – Alternative Vehicle License Plate Displays.

Chapter 3 License Plate Reader Fundamentals

Introduction

This section provides an overview of License Plate Readers (LPRs), the license plate reading process, and key challenges faced by LPR systems.

Typical applications for LPR technology by law enforcement, motor vehicle administrations, and other entities include but are not limited to:

- Law enforcement stolen vehicle and other "hot list" files
- AMBER, BLUE (violent criminal who has killed or injured a law enforcement officer), and SILVER Alerts
- Open road tolling (pay by plate)
- Congestion pricing
- Parking enforcement
- Access control
- Traffic studies
- Automated speed enforcement
- On-street parking enforcement
- Travel or journey time calculations

As the demand for LPR systems expands in both law enforcement and commercial applications, LPR technology continues to evolve. LPR provides cost-efficient approaches in varied environments that include both environmental challenges (e.g., mobile-based platforms, high-speed traffic) and license plate challenges (e.g., introduction of new designs, fonts, and so on across multiple jurisdictions).

The reads from LPR systems, namely the license plate number and in some applications the license plate jurisdiction, are primarily used as input into downstream systems to support the intended application. For example, whereas in open road tolling systems, the license plate number and jurisdiction are used to support the collection of toll revenues, in federal and state law enforcement systems, the license plate number and jurisdiction are used to support law enforcement queries against both large-scale (e.g., National Crime Information Center) and local data sources.

In some applications, manual verification or certification of LPR results is required at some point in the process. To the extent LPR systems can improve and retain a high degree of accuracy, operational costs can be reduced. In some applications, LPR system service-level objectives call for a 95% accuracy rate in correctly identifying both the license plate number and jurisdiction when the license plate is completely visible in the license plate image. The most significant challenge to maximizing license plate read rate accuracy is the ability of LPR system vendors to quickly adapt to the introduction of jurisdictional license plate designs with varying fonts, graphical designs, stacked letters, and so on.

License Plate Reader Systems

LPR systems include deployment of fixed, portable, mobile, and mobile application platforms.

Fixed Platforms

Fixed LPR platforms are permanently mounted on fixed infrastructure such as overhead gantries or roadside bollards. LPR fixed platforms are commonly used in open road tolling, commercial vehicle weigh station operations, and some federal and local law enforcement applications.



Fixed LPR in weigh station operations.



Fixed LPR in Customs and Border Protection inbound.

Portable Platforms

Portable LPR systems can be transported between locations, assembled, operated, and then disassembled. Once deployed, they operate as a fixed platform. Examples include portable trailers, traffic barrels, and other platforms configured with or containing LPR equipment.



Portable department of transportation trailer with LPR.



Speed trailer with LPR.

Mobile Platforms

Mobile LPR systems are defined as any LPR system that is mounted on a vehicle, whether a police car, tow truck, street sweeper, parking enforcement vehicle, and so on. These systems can include one to four camera configurations and are typically mounted on the roof or trunk, or they are custom manufactured.

Typical components of mobile systems include cameras that obtain images of the plate and vehicle, which in turn are passed to a processor mounted in the trunk. The processor locates the license plate in the image and extracts the license plate number. It then compares the textual license plate read against selected data sources and sends the output in the form of an alert to a mobile data terminal (screen) and an operator in the cab. The alert typically contains the name of the data source to which the image was compared such as an expired license or registration system, an infrared (IR) image of the license plate, and a color overview image of the vehicle in question. Data generated from mobile LPR systems can also be stored or transmitted via a back-office software application.



Patrol vehicle roof-mounted LPR.



Parking enforcement roof-mounted LPR.

Mobile LPR Applications (Apps)

Mobile LPR applications are defined as LPR systems that are held and operated by individuals using devices such as barcode readers, ruggedized PDAs, and smart phones that provide other capabilities (e.g., communications, internet access). These technologies provide mobile LPR capabilities and rely on the user to point the imager toward the location of the license plate.



LPR application on a mobile device.

Use of these devices is limited to speed applications typically less than 45 mph and are subject to unique challenges such as shadows, low ambient light, distance or angle to the license plate surface, and non-reflective surfaces. These limits can be overcome using techniques to light or IR illuminators resident in the device. Because IR imagers are not typically available on commercial general-purpose handheld devices, overcoming readability of non-reflective surfaces using a color imager generally requires special Optical Character Recognition (OCR) techniques. The accuracy of these OCR devices is dependent on the specific device and environment in which it is being used.

Handheld platforms are useful because they are easily deployed and can be used in parking enforcement, covert applications, portable checkpoints, and more. Benefits include portability, relatively low cost, and tactical use. The biggest drawback is that when the LPR application is used, it drains the device battery much faster than normal usage.

LPR Camera Technology

Two primary approaches are used to capture images from which the license plate information can be extracted. One approach is to capture a single still image of the license plate at an "optimal" distance from the camera, where the illumination, lens settings, and field of view can all be controlled to yield the best possible images under any ambient lighting and weather conditions. Another approach is to capture multiple images as the vehicle travels through the field of view of the camera. In this approach, near-instantaneous adjustments to the flash, shutter, and gain settings are performed to optimize the license plate image for different environmental conditions.

Monochrome (black and white), color, and IR cameras are used in various solutions. Monochrome cameras tend to yield the best resolution, can work with most types of visible light illumination, and are generally less costly. Color cameras are useful when the color information can be used to improve

the separation between characters and background and for identification of the jurisdiction. Color cameras require white light to produce accurate color information and are of very limited value at night without the use of additional illumination.

IR cameras are tuned to respond to IR illumination. IR cameras tend to be most sensitive at night and tend to be fitted with a band-pass filter designed to block visible light (to limit the effect of headlights and sunlight). This tuned IR illumination is effective at reflecting off the reflective background finish of the plate and not reflecting off the non-reflective characters (or vice versa).

Additional cameras are often used as part of the solution so that both a plate image and a vehicle image can be simultaneously captured to provide context and for investigative purposes. Multiple cameras are also useful when multiple bandwidths of light are used. For example, the fusing of white light and NIR (near-IR) light imagery adds significant information during the OCR and jurisdiction determination.

License Plate Recognition Process

The license plate recognition process begins when a vehicle is detected by an LPR system and ends when an LPR system information has been collected, analyzed, and handed off to backend systems for further processing.

The key steps of the LPR process are to

- Detect the vehicle and/or license plate.
- Locate the license plate in the image(s).
- Extract license plate characters from the background.
- Identify the license plate number.
- Determine the license plate jurisdiction *(optional).*
- Hand off LPR results to backend systems.

The following paragraphs describe each of the LPR steps in detail.

Detecting the Vehicle and/or License Plate

External triggers such as through-beam IR sensors, retro-reflective license plate sensors, ground-based induction loops, laser range sensors, and so on can be used to detect the presence of a vehicle in the field of view of the ALPR system. These types of triggers are primarily used in fixed-platform ALPR systems. Alternatively, the ALPR system detects the presence of a license plate by analyzing the camera's video signal (which may capture up to 60 images per second) and looking for potential license plate candidates. This type of detection is primarily used in mobile platform ALPR systems and can support vehicle speeds up to 140 mph. When the vehicle is detected, the ALPR captures one or more images containing the license plate that will be used to support the subsequent license plate number and jurisdiction determination.

Locating the License Plate in the Image

After one or more images containing a license plate are captured, a "license plate finder" algorithm is used to determine the exact location of the license plate in the image. This may be accomplished by searching for license plate characteristics (e.g., high-contrast objects) or character strings in the image that indicate the presence of a license plate. This process is one of the most difficult steps of the LPR process because the license plate must be located in potentially conflicting images that contain other information that may appear as license plates (e.g., bumper stickers, other writing, contrasting graphic designs). In addition, the type and condition of the license plate (e.g., retro-reflective, non-reflective, license plate frames and covers, license plate orientation) may require the use of special lighting and camera technologies to both locate and present the optimal license plate image to the character recognition algorithms.

As shown in the picture below, LPR cameras can vary flash, shutter, and gain settings to capture multiple images per vehicle over a wide range of ambient and environmental conditions.

Camera Arrangement	Resulting Image with Unchanged Ambient Conditions
Flash Duration = 130 µs Shutter Duration: = 200 µs Gain = 2	
Flash Duration = 390 µs Shutter Duration: = 500 µs Gain = 2	
Flash Duration = 780 µs Shutter Duration: = 1000 µs Gain = 2	

By varying camera settings and controlling illumination, the ability to locate a license plate within an image can be greatly improved. In addition, the 'best' image can also be used to improve the accuracy of the subsequent character extraction and license plate number determination.



License plate that has been located in the larger vehicle image captured by an LPR camera.

Extracting the Characters from the Background (Segmentation)

After the license plate is identified in the images(s), the region around the license plate may be further analyzed to extract the characters from the background. In the following example, pixels making up the candidate region are separated into foreground and background pixels to provide a more suitable candidate image used by the OCR algorithms to translate a character string image into an alphanumeric value that constitutes the license plate number. This is made more difficult when there is little contrast between the license plate number and the plate background.



The segmented or pre-processed license plate image is then passed off to OCR software, where the images are converted to individual alphanumeric characters.

Determining the License Plate Number

Challenge: Poorly designed fonts and variations in fonts themselves, additional symbols, half-height characters, location of registration stickers, license plate frames and covers, and holograms on characters all increase the complexity of OCR algorithms used to determine the alphanumeric characters of a license plate.



In the following example, you can see the software cannot discern whether the first character is a "B" or and "8" and whether the third character is a "6" or a "G."

In the following license plate examples, the ascender and descender of the letter 'Q' takes on different characteristics that may require specifically tuned or trained OCR engines depending on the region or jurisdiction in which the LPR system is deployed. The number '4' in the first license plate compared with the '4' in the second photo below provides another example of inconsistent fonts used between jurisdictions, making the same number look different. Note that the image processing and segmentation steps described must discern the actual license plate number from other alphanumeric information such as vehicle registration tabs and jurisdiction names and logos.





Determining the License Plate Types and Jurisdiction

Some LPR systems can identify the license plate type and the jurisdiction of origin by recognizing key features on the plate such as the jurisdiction logo, background graphics, special symbols, unique character font features, and so on. Other techniques include applying syntax rules and other regionalization rules to provide additional clues to determine the license plate jurisdiction. Use of white light for this process significantly improves the accuracy of jurisdiction identification. Many of the jurisdiction specific features are lost when imaging the license plate in the NIR light spectrum.



Handing Off LPR Results to Backend System

After the license plate number and, in some cases, the jurisdiction, are determined, the information is handed off to backend systems in support of the intended LPR system application. These systems may compare the license plates with watch lists or other law enforcement systems to allow interdiction or other actions to occur in near real time. Sometimes these actions are not for interdiction purposes but merely to allow vehicles to gain access to secure locations, parking garages, and so on.

In some cases, the LPR data—along with supplemental data such as scene and driver images, vehicle location, and date and time stamps—are stored in highly scalable and searchable data sources to support intelligence analysis, bill generation, or other processes that may occur at a later date.

LPR systems are often configured to automatically communicate or transmit all the collected data to a backend data archive or server. Communication methods can include any conventional networking protocols, including cellular, Wi-Fi, hardwire, and thumb drives, all with a variety of security protocols. In many cases, this communication process occurs in the background without any effort from the system user.

After the data have been inserted into the backend data management software, they are immediately available for review and search. These systems are generally web based and can support numerous workstations simultaneously. Often the software solutions used to manage data sources allows information to be queried in a multitude of ways, by location, time, plate number, and so on.

In addition, the image captured and the results generated by the ALPR system can be digitally signed and encrypted to enable a third party to verify that the data was collected at a specific time and location and that no one has tampered with it. This approach also provides for a chain of custody for legal evidence purposes.

Challenges Associated with License Plate Reading

Certain steps of the LPR process present unique challenges that require continuous innovations in hardware and software technologies. A key challenge is the constant introduction of new and varied license plate designs that greatly expands the types of license plates

that LPR systems are required to process. Some of those challenges and the current techniques being applied to address these challenges include the following.

Detecting the Vehicle and/or License Plate

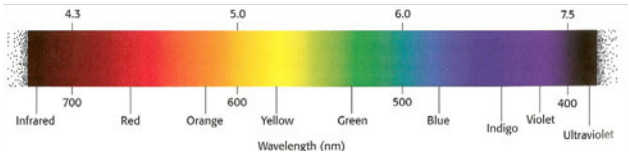
Challenge: LPR systems operate in outdoor environments subject to constantly changing conditions, including lighting, weather, varying vehicle speed and acquisition angles, and varying distances from cameras.

Techniques: LPR camera locations, focal points, illumination controls, and vehicle detection sensors are carefully controlled to help ensure the capture of optimal images used for subsequent license plate location and OCR. Often ALPR cameras are sequencing illumination levels or acquisition parameters to counteract the constantly changing conditions in which they are operating.

Locating the License Plate in the Image(s)

Challenge: Low-contrast license plates, license plate frames and covers, and other noise in the image (e.g., bumper stickers) all impact the ability of license plate detection algorithms to locate the license plate in the larger image captured by the LPR system.

Techniques: Commercial LPR systems typically use a narrow band of IR illumination to light the plate for detection purposes in nearly all weather and lighting conditions. This band ranges from 750 nanometers (nm), which has a visible bright red glow, to 810, 850, 940, and 950 nm. A 950-nm IR illumination is completely invisible to the naked eye.



The purposes in using several bands of IR light are to filter out the effects of background graphics and to highlight the alphanumeric characters for OCR software systems. To help overcome graphic-heavy backgrounds, a spectral analysis can be performed automatically on a plate-by-plate basis to determine which IR illumination is best suited for each plate at the time it is read by the LPR. In general, lower IR bands such as 750 nm handle heavier graphics, and higher IR bands of light are more effective with lower density graphic backgrounds.

Extracting License Plate Characters

Challenge: License plates with conflicting backgrounds or graphics that encroach on the character fields present conditions that make it difficult to recognize specific license plate characters.











Technique: To address these challenges, LPR systems can use different illumination techniques to improve the contrast between characters and background. Also, specialized segmentation algorithms are used to segment the characters from the background. Many LPR systems use neural networks that are trained to find characters correctly in cases of low contrast between characters and background.



In this example, the R could be read as an A and the Q as an O.





The first photo shows a plate with three stacked characters (the AAMVA License Plate Standard calls for no more than two characters to be stacked). The second photo shows appropriate half-height stacked characters. In some jurisdictions, the stacked characters are considered part of the plate number, but in other cases, they are not.





When characters are located too close to the plate's edge, license plate frames can easily prevent the plate number from being read by an LPR.

Chapter 4 License Plate Reader Benefits

Introduction

Prior to the introduction of License Plate Reader (LPR) technology, a law enforcement officer could run a minimal number of plates per shift. LPR technology allows an officer to "read" more than eight times the license plates than officers conducting only manual checks. LPR systems may be used in targeted areas such as crime hot spots, assisting law enforcement in obtaining valuable information of vehicles that may be involved in criminal activity. Moreover, by eliminating the manual check process, not only is officer efficiency increased, but it allows officers to focus more on their surroundings, which improves both officer and public safety.

In studies supported by the National Institute of Justice, research was conducted as to the effectiveness of LPR use for law enforcement patrol and investigations. The first study was conducted in a large suburban jurisdiction in designated hot spots for a period of four months. Officers who used LPR were found to be much more likely to recover stolen vehicles than officers who did not use LPR. The second study examined how LPR could be used for investigations and was focused on a large city with nearly 100 LPRs in fixed locations. After two years, researchers noted 4,000 incidents were documented, including auto theft, missing persons, and homicide cases. LPRs were found to provide information that contributed somewhat to resolving roughly one in five incidents.[1]

Misreads of license plates by LPRs or illegible license plates causing no reads by LPRs do occur.

1 Christopher S. Koper and Cynthia Lum, "Effectiveness of License Plate Readers for Patrol and Investigations," Research in Brief, Police Chief 85, no. 9 (2018): 14–15.

Research conducted by one major toll authority from December 2020 indicated that 9% of toll revenue was lost because of unbillable revenue from misread or illegible license plates.



Gantry mounted LPR technology commonly used for automated toll collection.

When they do occur, the potential for arresting the wrong person, missing an opportunity to arrest a suspected criminal or terrorist, recover a stolen vehicle, or miss toll revenue exists. Research conducted by one major toll authority from December 2020 indicated that 9% of toll revenue was lost because of unbillable revenue from misread or illegible license plates.[2]

Challenges to Law Enforcement

In the past, a law enforcement officer could be familiar with all 50 states' license plates. Today with the proliferation of license plate designs, specialty, and vanity plates—in some cases into the hundreds in a single jurisdiction—it is virtually impossible for instant visual recognition for today's police officer. The issue

2 E470 Public Highway Authority Quarterly Dashboard Report December 31, 2020.

is exacerbated by the introduction of additional new license plate designs each year. Moreover, novelty plates that closely resemble official license plates have added to the difficulty law enforcement contends with in determining plate validity.

A sampling of eight states illustrates the significant growth in the number of license plate designs in circulation in the U.S.

This table represents a sample of the growth in license plate designs:

Jurisdiction	2009	2012	2021
Arizona	52	64	75
California	106	117	167
Maryland	800	935	1,365
Missouri	172	200	269
Montana	152	177	350
Pennsylvania	245	310	582
South Carolina	385	417	429
Texas	225	376	499
8 state totals	2,137	2,596	3,736
% Increase from 2009 to 2021			57%

Officer Safety Benefits

Safety is of paramount concern for any law enforcement officer initiating a "routine" traffic stop. Officers in patrol vehicles that are not equipped with LPR technology may not be as informed about the vehicle and its occupants as those who have the technology.

LPR technology provides the ability to check the vehicle plate number automatically and rapidly against selected databases. License plates are often "flagged" when the owner is associated with certain information (e.g., wanted, attempt to locate, be on the lookout for, stolen car). With LPR technology, officers stopping drivers for sometimes minor traffic offenses can be made aware of this type of information, which allows them to use the appropriate officer safety tactics given the information they have instead of unknowingly walking into a dangerous encounter.

Traffic Safety Benefits

One significant example of a traffic safety benefit involves suspended, *revoked, or otherwise ineligible* drivers. *Across North America, at any given time, approximately 7% of all drivers are suspended, and it is estimated as many as 75% of these people continue to drive.*[1] Moreover, 19% of all fatal crashes involve an unlicensed or suspended driver. These drivers pose a significant threat to highway safety. LPR technology has the capability to quickly identify vehicles whose registered owners have suspended or revoked licenses or registrations, making it much faster and easier for law enforcement officers to detect and apprehend suspended drivers.



Benefits to Law Enforcement: Beyond Traffic Safety

LPR's are at the forefront of discussions about the impact of technology on improving traffic and public safety. In the field of auto theft recovery and investigation, the LPR is a force multiplier for officers in the field. The technology enables reading and checking the status of thousands of license plates in a single shift, all while the investigator can watch his or her surroundings for activity, malevolent or benign. The LPR is a tireless partner, constantly on the watch

1 The National Cooperative Highway Research Program, Report 500, Volume 2.

for stolen vehicles and wanted subjects, AMBER Alerts, missing persons, and more. This technology is even more effective when there is a front and rear license plate for the LPR to read.

Many police agencies use LPR-equipped vehicles to collect plate information as they respond to bank robberies and other major crimes to capture plate numbers of vehicles leaving the area as police respond to the scene of the crime. There have been many instances when these reads have led to the identification of suspect vehicles and suspect arrests.

Public Safety Benefit

As mentioned in the previous Benefits subsections, LPR-equipped law enforcement vehicles can scan thousands of plates an hour, thus increasing the chances of finding a particular vehicle quickly, enhancing highway and public safety. One example was provided by the Utah Department of Motor Vehicles Enforcement Division, which prior to installing LPRs on their police vehicles, averaged



One example was provided by the Utah Department of Motor Vehicles Enforcement Division, which prior to installing LPRs on their police vehicles, averaged 400 stolen vehicle recoveries annually. After LPR deployment, they now scan 45,000 plates monthly and are now recovering more than 1,000 stolen vehicles annually. See Chapter 7 – License Plate Reader Success Stories for many more examples.

400 stolen vehicle recoveries annually. After LPR deployment, they now scan 45,000 plates monthly and are now recovering more than 1,000 stolen vehicles annually. See Chapter 7 – License Plate Reader Success Stories for many more examples.

It should be noted that there are circumstances when the lack of a front license plate limits the effectiveness of LPR on front-facing traffic. This is also an issue for school bus drivers who report drivers who fail to stop for the buses while loading or unloading students. These drivers often rely on the presence of a front license plate to be able to report these violations. Some tolling authorities also rely on the front plate for both revenue collection and enforcement.

Homeland Security Enhancements

LPR technology has also become an important national security tool. LPR technology is used to query the license plate numbers of vehicles entering and departing the U.S. to identify potential threats to national security. LPR units are also set up in locations in proximity to critical infrastructure to identify potential threats.

Chapter 5 License Plate Readers as a Tool to Improve Toll, Commercial Motor Vehicle, and Border Operations

Introduction

This chapter discusses how License Plate Reader (LPR) systems benefit public mobility but also have become core to the way many electronic toll systems collect tolls and enforcing payment. LPR has made it possible for the toll industry to move increasingly toward all-electronic cashless toll operations, which are permitting free-flow traffic to pay tolls at highway speeds, improving roadway efficiency, improving the customer experience, and mitigating adverse environmental impacts. Road and bridge toll collection helps provide revenue assurance for highway lane management, maintenance, and improvement.

LPR systems are also effective in commercial vehicle enforcement, which results in efficiencies in safety and traffic flow near weigh station and inspection facilities. These systems help officers identify and focus resources on the vehicles and drivers that are most likely to present safety risks.

LPR systems are also deployed by Customs and Border Protection along the U.S. borders with Canada and Mexico to improve and enhance traveler mobility across these borders.

The introduction of electronic toll collection (ETC) has reduced the dependence on toll collection personnel and manual cash transactions at toll points. Although ETC has improved traffic flow and efficiency, it has also introduced a new challenge—toll evasion and revenue loss.

Mobility and Toll Collection

Collection of user fees on roads, bridges, and tunnels—or tolls—has served as an important means of financing key transportation projects and funding ongoing operations and maintenance for as long as roads have existed. Tolls provide a direct approach to funding highways, bridges, and tunnels without increasing local or state taxes, and they ensure that those who use and benefit the most from these projects pay for them directly.

For toll facilities to be effective, however, tolls must be collected. Historically, toll collection involved staff at a gate or in a toll booth collecting cash directly from motorists and making change at strategic points along the roadway. This process required each vehicle to stop in the tolling zone for a brief period to tender a cash toll payment. When the collection site becomes a choke point – risks of rear impact and chain reaction crashes increase. Toll chokepoints also reduce the efficiency of the corridor where collection takes place. Additionally, when toll collection slows traffic, the reduced efficiency adds emissions into the environment and increases the time required to move people and commercial goods.

Over the past three decades, most toll operators modernized their toll collection systems with technology that allows for prepaid toll accounts using in-vehicle transponders to identify valid toll account holders. The introduction of electronic toll collection (ETC) has reduced the dependence on toll collection personnel and manual cash transactions at toll points. Although ETC has improved traffic flow and efficiency, it has also introduced a new challenge—toll evasion and revenue loss. Toll violators

include motorists who travel through an ETC-only lane without a transponder or unfunded toll account, creating unpaid toll transactions. This not only reduces the funding available for roadway operations and maintenance but also adversely affects fairness to those who pay their tolls, potentially eroding public support for tolling. In an ETC environment, there is a cash payment option for motorists without a transponder and prepaid toll account. LPR technology is used to capture license plate images of vehicles without toll transponders in ETC toll lanes to enforce the toll payment from the registered vehicle owner.

In recent years, toll operators are increasingly adopting all-electronic tolling (AET) operations, in which the cash payment option is eliminated entirely. Cashless AET operations offer the benefit of allowing free-flow tolling, often permitting all vehicles to move through the tolling point at the posted speed limit without stopping or slowing. AET operations are reducing the need to separate cash payment and ETC vehicles and the associated roadside infrastructure required to do so. Instead, AET operations often use overhead gantries with electronic toll equipment (e.g., antennas, transponder readers, and LPR cameras) to process the toll transaction with all vehicles.

This not only reduces the funding available for roadway operations and maintenance but also adversely affects fairness to those who pay their tolls, potentially eroding public support for tolling.

Vehicles with in-vehicle transponders pay their tolls through their toll accounts, just as they do in an ETC environment. Vehicles without toll transponders in an AET environment have their license plate images captured, and toll bills are sent to the registered owners of the vehicles to arrange payment of the toll due. In an AET tolling environment, more transactions are being processed based on LPR technology. For commercial motor vehicles, the Federal Motor Carrier Safety Administration estimates a truck will save approximately $10 per facility each time a truck is able to legally bypass a weight station or inspection facility.

Today as motor vehicle transportation solutions orient their designs toward improved mobility, reduced congestion, and more reliable levels of service, the use of LPR technologies has increased substantially. The conundrum in this development is that as LPR technologies improve, license plates continue to take on increasingly complex designs, making accurate license plate reading problematic.

According to the Federal Highway Administration (FHWA), jurisdictions throughout the U.S. are installing managed lanes (e.g., high occupancy/toll [HOT] lanes) in response to increased congestion. Managed lanes are intended to lessen congestion and provide greater mobility than the adjacent general-purpose lanes of state highways or interstate highways located in urban areas. In some cases, it is also used to enforce High Occupancy Vehicle (HOV) violations automatically, without the need of a law enforcement officer to visually detect violations. LPR also assists transportation officials to understand and influence traffic patterns and set flexible pricing based on traffic levels to reduce congestion, resulting in fewer roadway incidents and increased mobility.

Today as motor vehicle transportation solutions orient their designs toward improved mobility, reduced congestion, and more reliable levels of service, the use of LPR technologies has increased substantially. The conundrum in this development is that as LPR technologies improve, license plates continue to take on increasingly complex designs, making accurate license plate reading problematic.

Another feature of the move to LPR-related open road tolling is the use of enforcement-intended data access for revenue collection that is not law enforcement related. In jurisdictions where overhead tolling is

introduced, the department of motor vehicles should be consulted in the means by which vehicle and vehicle operator data may be obtained.

Revenue Loss

License plate designs, license plate obstruction, and purposeful avoidance to register and title vehicles are the most significant contributors to revenue losses for authorities using LPR systems. License plates that align with the AAMVA License Plate Standard will improve the effectiveness of LPRs and subsequently increase toll collections.

One toll agency with years of experience in operating a cashless AET operation that depends on license plate images to collect tolls from motorists without toll transponders indicates the following experience:

	2017		2018		2019	
Total Image Transactions	36.930M		39.092M		41.143M	
Reject Reason	Total	%	Total	%	Total	%
Unreadable Plate	2.058M	5.6%	2.139M	5.5%	1.901M	4.6%
Temporary Plate	1.063M	2.9%	723K	1.8%	667K	1.6%
No DMV Record	1.116M	3.0%	801K	2.0%	780K	1.9%
Other	784K	2.1%	1.061M	2.7%	978K	2.4%
Unenforceable Totals	5.021M	13.6%	4.724M	12.1%	4.326M	10.5%
Lost Revenue	$23.1 Million		$25.8 Million		$25.3 Million	

Although the unrecoverable revenue is significant, it should also be noted that even through a 12.1% growth in image-based transactions over three years, there was a 13.8% decline in unenforceable images. This is indicative of what the industry has experienced in terms of improvements in hardware, software, and business practices improving overall outcomes. That said, easily identifiable license plates can further mitigate lost revenue in the transportation industry as well as other businesses and enforcement models that use imagery and license plate information as the core of their revenue enforcement efforts.

Lost toll revenues amounted to $23.1 million in 2017, $25.8 million in 2018, and $25.3 million in 2019.

Mobility at U.S. Borders with Canada and Mexico

Currently, Customs and Border Protection (CBP) has three programs that use LPR to expedite entry to the U.S.—NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Free And Secure Trade (FAST). NEXUS is used at the Canadian border and SENTRI, is used at the Mexican border. FAST is a commercial clearance program for low-risk shipments entering the U.S. from Canada and Mexico. Each of these programs has dedicated lanes, and users are vetted.

All vehicles and persons entering the U.S. are subject to inspection. Every vehicle and every person entering at a land border port must be queried through various law enforcement databases before they can enter the U.S. Although the inspection process encompasses more than just queries, each query takes time to perform, and time is a factor in vehicle wait times. CBP, through the Western Hemisphere Travel Initiative (WHTI), has installed technology at most ports of entry that automates many functions previously done manually. This automation has resulted in reduced vehicle inspection times while maintaining the integrity of the inspection process.

Other LPR Applications That Benefit Mobility

Commercial Vehicle Enforcement

Commercial Vehicle Enforcement entities use LPR. Several specialized companies have emerged that use LPRs to read license plates and compare the plate number to federal safety data sources to ensure trucks are in compliance with federal and state motor carrier safety programs. Some systems also verify various state and federal credentials required to operate in the jurisdiction, check for out-of-service violations, and check for wants or warrants associated with vehicles.
Municipal Parking Enforcement



LPR camera in use at a roadside truck scale.

Municipal Parking Enforcement

On-street parking enforcement efficiencies have been gained by using LPR technology. With these systems, parking scofflaws who fail to pay their parking citations or fines are placed in a data source that is downloaded to an LPR-equipped vehicle. The LPR quickly identifies those who have failed to pay, which allow municipalities to boot vehicles, ensuring parking revenues are recaptured.



Mobile LPR camera mounted on parking enforcement vehicle.

In a 30-day trial conducted during 2020 using one LPR-equipped vehicle, the Long Beach Police Department in southern California identified nearly 300 scofflaws who had five or more unpaid parking citations, capturing nearly $200,000 in unpaid fines. In addition, seven arrests not associated with a parking citation were made.

Chapter 6 License Plate Reader Program Best Practices for Law Enforcement

Introduction

A properly organized and managed license plate reader (LPR) program can greatly enhance the effectiveness of patrol operations and criminal investigations. The best LPR programs are built on a foundation of good policy and training.

The measurement of success for an LPR program is subjective. Recovering stolen vehicles; arresting subjects with active warrants; and recovering AMBER, SILVER, and BLUE Alert subjects are some measures of success. However, in an era of transparency and civilian oversight, a true measure of success should include an agency's ability to collect, store, and delete millions of LPR reads in an efficient and secure manner. It should also be noted that LPR systems are only as good as the data they rely on. Ensuring that the hot lists they access are kept current is critical to limiting the possibility that users will act on erroneous information.

Policy

Law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety. Policies should include LPR program goals and objectives and should not be too restrictive as to limit 'operators' ability to perform law enforcement functions yet still be protective of the massive amounts of data an LPR system collects.

Because LPR equipment and accounts can have broad permissions, policies should contain language defining what functions an operator can and cannot perform with an assigned LPR account or LPR equipment. Having operators sign an acceptable use statement is a method of tracking and ensuring each user has been made aware of the policies set forth. In addition to the policies already explained, the following specific topics and their relationship to the use of LPRs should also be reflected in policy:

- **Data retention and dissemination** – Data usage policies should conform with jurisdiction laws governing the agencies legal authority to collect, retain, disseminate, and dispose of LPR data. Agencies should have a data retention period in policy (whether it is included in jurisdiction law or not) with justification for the data retention period they choose.
- **Freedom of Information Act (FOIA)** – An agency's FOIA policy should be examined to reflect the legal standards of FOIA.
- **Data security** – Operator passwords, system lockouts, system audits, and user audits should all be addressed in policy. Many of these are already established within an agency or by an overarching governing body. Assurances should be made to maintain compliance with these existing policies.
- **Memorandums of understanding (MOU)** – Many agencies and jurisdictions may decide to work together to establish one large LPR network. This reduces the cost per agency, and the burden of responsibility is shared. An established MOU identifies the roles and responsibilities between the agencies.

See Appendix (C) for Sample LPR Policies from Ohio, Utah, and Virginia.

Training

In addition to having sound policy, formalized training should be in place that conveys the policy content to LPR system operators. Training is a fundamental component of an LPR system. Without properly documented training, operators have no direction for which to properly set up, use, and troubleshoot LPR equipment. Training should emphasize policy (and case law) surrounding data retention. This can serve to assure the public that data are being collected, stored, used, and deleted in a manner consistent with established legal guidelines and policy.



LPR training can be divided into three sections: operations, data analysis, and technical support. All sections of training should be recurring and culminate in a test. This ensures new material is presented and operators remain vigilant in the use of the LPR system.

Operations training should focus on the daily operator of an LPR-equipped vehicle. Like speed-measuring devices, the operator of an LPR-equipped vehicle should be able to set up, operate, and troubleshoot a vehicle-mounted LPR system.

Data analytics could be considered the second most important function of an LPR system.(the most important function being data collection). Having the training necessary to analyze a target vehicle across a network of LPR cameras relies on consistent and thorough training.

The last section of training which that be included in an LPR program is technical support. This section of training encompasses the logistical support staff most agencies will use to up-fit LPR patrol vehicles, monitor fixed sites, perform server maintenance, and perform system upgrades.

LPR Program Staffing

An LPR program should be adequately staffed to provide proper program support, oversight, and planning. Prior to determining staffing levels, a decision should be made if the LPR program will fall under the management and leadership of an existing police hierarchy (such as Operations or Investigations) or if it will be autonomous (specialty unit).

If an agency has fixed LPR equipment in its program, the program should be staffed sufficiently to maintain 24-hour operations to respond to any received alert, such as AMBER Alerts.

An LPR program needs enough employees to install and fix the equipment and employees who can manage both the system and equipment. If agency staffing is limited, employees can effectively multitask and meet the needs of multiple positions at once. If an agency does not have the number of employees or expertise to complete all the required aspects of running an efficient program, contractors can be employed to conduct one or more critical functions of the LPR program.

Equipment

Like staffing, LPR equipment needs to encompass all aspects of the program. A comprehensive, but non-inclusive list of equipment needed for an effective LPR program follows (mobile, fixed, and portable platforms):

MOBILE LPR	FIXED-SITE LPR	PORTABLE PLATFORM
Vehicle-mounted readers	Overhead or pole-mounted readers	Platform: commonly a trailer
Connecting wires from readers to trunk box	Continuous power supply	Continuous power supply (solar combined with battery)
Trunk box	Cellular or fiberoptic network	Cellular network
Mobile systems software	Systems software	Systems software
Mobile computer capable of operating mobile systems software		
GPS-capable antenna		



Vehicle-mounted reader.



Pole-mounted reader.



Trailer-mounted reader.



Roof-mounted LPR.



Trunk-mounted LPR.

There are many LPR manufacturers that produce reliable and durable LPR equipment. Purchasing agents need to consider the proprietary nature of LPR equipment and be aware that some products are not interoperable with others. It is critical for LPR data to properly communicate from the point of collection

(reader) to a central computer (server). LPR data must be securely protected and accessible by operators, most commonly from a desktop- or vehicle-based computer system. Legal considerations need to be addressed before purchasing equipment. For example, a cloud-based data storage system may not be compliant with a jurisdiction's data storage laws.

The specific type of LPR equipment chosen should be driven by agency mission and priorities. Whereas some agencies may prefer only mobile LPR, others may also use fixed-site LPR's, covert equipment, or portable platforms to create a robust LPR program.

When selecting LPR equipment, anticipate and plan for program expansions and logistical support needs. Items such as spare parts, storage facilities, and ancillary equipment should be considered as well.

Summary

A well-thought-out and well-executed LPR program provides law enforcement an additional tool in providing essential public safety services. Establishing an LPR program is a task that should be completed with careful consideration, planning, and organization.

Chapter 7 License Plate Reader Success Stories

Introduction

What follows are documented examples of how License Plate Reader (LPR) technology has benefited law enforcement in the performance of their public safety mission.

On **January 7, 2021**, Kristin Walker from Alabama was putting fuel into her vehicle with her two children in the backseat when a subject jumped into the driver seat to steal the vehicle. Walker was able to remove her children from the vehicle before it was highjacked. With the use of LPR technology, the Rankin County, Mississippi, Sheriff's Office was able to spot the vehicle a short time later and arrest the two subjects involved.

In **December 2020**, a North Carolina DMV License & Theft Bureau Law Enforcement Agent observed a Volkswagen traveling in a toll lane at a high rate of speed and attempted to stop the vehicle. The vehicle operator failed to stop, and with speeds near 130 mph, the pursuit was called off. LPR information was obtained from the North Carolina Turnpike Authority that included photographs of the driver, vehicle, and license plate information. The violator was located, apprehended, and charged with several serious traffic violations.

On **December 19, 2019**, A Delaware guidance counselor allegedly sexually assaulted a minor teenage boy while in Ocean City, Maryland. The victim alleged Allen Reese drove him from Delaware into Ocean City, where he sexually assaulted him. Using Ocean City's LPR, detectives were able to confirm that Reese's vehicle crossed the Route 90 bridge as well as entry and exit times consistent with the dates and times of the assault provided by the victim. Based on the evidence from the victim corroborated by the LPR system, detectives scheduled an interview with the suspect to execute a warrant and collect DNA samples. However, detectives were notified by Homeland Security that a flight to Casablanca, Morocco, had been booked for Mr. Reese. Because it appeared that he was preparing to flee the country to avoid the sexual assault charges, a warrant was immediately issued for Mr. Reese. He was quickly located and held without bond on charges of sexual abusing a minor and third-degree sexual offense.

In **August 2019**, police with Duck, North Carolina, Police Department (an Outer Banks Island community) deployed their LPR systems to find residents who stayed on the island during a mandatory evacuation during Hurricane Dorian. LPR cameras recorded the plate numbers of vehicles exiting the island to determine which registered vehicles did not leave. The homes associated with those vehicles were visited by police to warn those residents of the risks of remaining on the island.

On **July 24, 2019**, a woman put her dog Happy into her car in Baltimore's Guilford neighborhood. She was just getting into the driver's seat when she was forcibly pulled her from her car and several suspects got into her car and sped off. Happy was still in the car when the suspects fled. The woman notified police, and the Baltimore Police Department immediately placed the license plate on an LPR hotlist as a carjacked vehicle. Soon after a patrol officer passed by the vehicle, which

was parked and unoccupied, and received an alarm on the LPR system he was operating. He approached the car and saw that Happy was still inside with the windows closed and doors locked. Because it was a hot July day, the officer smashed a window and rescued Happy before he was overcome from the heat. The woman and Happy were soon reunited.

On **July 15, 2020**, a man shot and killed his ex-girlfriend in the parking lot of her workplace in Springfield, Tennessee. Two days later, the suspect drove through Mt. Juliet, where a Mt. Juliet Police Department (MJPD) vehicle equipped with an LPR system detected the suspect vehicle license plate, alerting the officers who arrested the suspect.

According to MJPD Chief James Hambrick, "It's amazing the stuff that you wouldn't know travels through your city … is actually traveling through your city." That's one of many success stories to come out of the MJPD's use of LPR, Chief Hambrick said.

On **June 30, 2018**, a subject in Sacramento, California, was attempting to cross a street in his wheelchair and was hit and killed by a passing motorist who failed to stop and render aid. The license plate belonging to the vehicle that left the scene was detected by LPR, and the driver was arrested for felony hit and run.

On **March 15, 2018**, James Allen Hayes plead guilty in federal court to committing multiple bank robberies over the course of five months throughout California. Hayes was apprehended as a result of LPR detecting his vehicle traveling between robbery locations.

Robert Sheets was accused of shooting a man on **August 13, 2017**, in Manor Township, Pennsylvania. Sheets returned to the suspect the next day and discovered him still alive. He then shot the victim again, leaving him for dead and fleeing the area. Miraculously, the victim survived and was able to identify the man who tried to kill him as Sheets. The vehicle driven by Sheets was immediately filed in National Crime Information Center as a felony vehicle, which resulted in a hotlist entry on LPR systems across the U.S.

A few days later, in Fairfax County, Virginia, an LPR alerted officers that Sheets was connected to a 2007 Ford Edge heading west on I-66. Fairfax police cruisers pulled in behind Sheets, and after a 38-mile pursuit, Sheets was apprehended.

On **August 26, 2015**, a gunman shot and killed a news anchor and cameraman from a local news station (Alison Parker and Adam Ward) while they were doing a report in Roanoke, Virginia. The license plate number of the shooter was broadcast statewide. Several Virginia State Police patrol vehicles were equipped with LPR. Five hours later and approximately 200 miles away from the shooting scene, Virginia State Police Trooper Pam Neff entered the license plate number into her LPR and discovered the LPR had just read the suspect license plate three minutes prior. Trooper Neff was able to catch up to the suspect vehicle and when back-up was in position proceeded with the apprehension. Trooper Neff was recognized by AAMVA during the AAMVA Annual International Conference in Williamsburg, Virginia, in August 2016.

For more news stories about law enforcement LPR successes from September 2017 to September, 2018, go to https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf

Appendix A Significant License Plate Reader Court Cases and Applicable Federal Statutes

United States Court of Appeals for the Ninth Circuit
United States v. Jay Yang,
958 F.3d 851 (9th Cir. 2020).
May 4, 2020
https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

Jay Yang was observed stealing mail from U.S. mail collection boxes on surveillance cameras driving a rented GMC vehicle beyond the rental contract due date. The license plate number was observed and searched in a License Plate Reader (LPR) database, which helped lead investigators to his home. Yang claimed because his rental agreement was past due and the contract was no longer valid when the plate was observed by LPR, the LPR data were invalid, and anything obtained from the search of his residence was not admissible. The court ruled there is no expectation of privacy of a license plate regardless if rental contract was expired. The LPR database did not reveal all the defendant's movements and therefore did not infringe on reasonable expectation of privacy.

United States Court of Appeals for the Eleventh Circuit
United States v. Larry Lamar Wilcox,
415 F. App'x 990 (11th Cir. 2011).
February 28, 2011
https://law.justia.com/cases/federal/appellate-courts/ca11/10-13031/201013031-2011-02-28.html

Larry Wilcox argued the use of LPR technology amounted to unconstitutional surveillance violating his reasonable expectation of privacy. The defendant said the district court erred in denying a motion to suppress, stating an Atlanta police officer's use of LPR technology violated his Fourth Amendment right to be free from an unreasonable search.

The Court of Appeals ruled that the Supreme Court had concluded in similar contexts visual surveillance of vehicles in plain view does not constitute an unreasonable search for Fourth Amendment purposes. Given the Supreme Court's Fourth Amendment precedent, the Court of Appeals ruled the district court did not commit plain error in concluding Wilcox did not have a reasonable expectation of privacy in the plainly visible license plate and the officers' use of LPR did not violate the Fourth Amendment.

United States Supreme Court
United States v. Knotts,
460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (U.S. 1983).
December 1983
https://supreme.justia.com/cases/federal/us/460/276/

Tristian Armstrong was being investigated for stealing chemicals to manufacture illegal drugs. Agents attached a radio transmitter to a container of chemical sold to Armstrong, which tracked the location of where methamphetamine was being produced by Leroy Knotts. A search warrant was obtained, and an illegal drug manufacturing lab was discovered.

Knotts was convicted in district court, but the U.S. Court of Appeals reversed the conviction, stating Knotts' Fourth Amendment rights were violated by use of the tracking device, and the evidence could be suppressed. The U.S. Supreme Court held the initial conviction, ruling the tracking device did not invade any legitimate expectation of privacy and was neither a "search" nor a

"seizure" by grounds of the Fourth Amendment. The movement of a person traveling on a public highway does not afford an expectation of privacy of the movements. Nothing indicated the tracking device was used to gather information from within the private area.

Privacy and Fourth Amendment

Authority for Police to Check License Plates
United States Court of Appeals for Ninth Circuit
***United States v. Ismael Diaz-Castaneda*,**
494 F.3d 1146 (9th Cir. 2007).
July 18, 2007
https://caselaw.findlaw.com/us-9th-circuit/1468527.html

An officer ran the license plate on a pickup traveling in front of him in traffic. The plate information response indicated that the driver's license of the registered vehicle owner, Solia Diaz, was suspended. The officer, believing the operator fit the description of Diaz, stopped the vehicle. Diaz was arrested for driving while under suspension. The vehicle passenger, Ismael Diaz-Castaneda, was found to have an immigration detainer on him and was arrested.

Diaz-Castaneda argued the stop violated his Fourth Amendment rights, and any subsequent evidence should be withheld. The court held a license plate check does not constitute a Fourth Amendment search, and evidence should not be suppressed.

U.S. Court of Appeals for Sixth Circuit
United States v. Curtis Ellison,
462 F. 557 (6th Cir. 2006).
September 5, 2006
https://caselaw.findlaw.com/us-6th-circuit/1031532.html

A Farmington Hills, Michigan, police officer ran a license plate of a parked vehicle through a police telecommunication system belonging on a vehicle operated by Curtis Ellison. Information returned revealed the registered owner was a "wanted person." Ellison was determined to be a passenger in the vehicle and was arrested. District court originally ruled the officer did not have probable cause to run the plate because the van was not parked illegally, and therefore Ellison Fourth Amendment Rights were violated. The court determined what a person exposes publicly is not subject to Fourth Amendment protection, and observing a license plate displayed in plain view does not constitute a search.

Validity of License Plate Reader Technology

United States Court of Appeals for the Third District
***United States v. Marcus White*,**
504 F. App'x 168 (3d Cir. 2012).
November 15, 2012
https://law.justia.com/cases/federal/appellate-courts/ca3/11-4035/11-4035-2015-04-29.html

Marcus White was convicted in Pennsylvania for his involvement in robberies of a post office and convenience stores. White's vehicle had been reported stolen and was detected by a Maryland state police trooper by an alert from an LPR while on patrol. During the suppression hearing, the District Court noted "the technology used by the license [plate] reader is verifiable and acceptable technology." White did not challenge this conclusion.

Use of License Plate Reader Data

Supreme Court of Virginia
Opinion of Justice Stephen R. McCullough
Harrison Neal v. Fairfax County Police Department, ET AL,
299 Va. 253, 849 S.E.2d 123 (Va. 2020).
October 22, 2020
https://law.justia.com/cases/virginia/supreme-court/2020/191127.html

In a prior ruling, the Virginia Court of Appeals ruled the "passive use" of LPR data by Fairfax County, Virginia, police violated the Virginia Data Act. Neal

argued the police department could not collect and store passively obtained LPR data without suspicion of criminal activity. Neal claimed the Virginia Data Act prohibited the gathering of personal information unless justified by law. The court initially ruled the LPR data provided a link to identify the vehicle owner and therefore LPR data was subject to the Virginia Data Act.

In a later ruling from the Virginia Supreme Court, the court stated the LPR system did not qualify as an information system because it did not contain name, personal number, or other identifying particulars of data for a subject. The court further stated the plate, vehicle photo, date, time, and GPS location did not bring the Data Act into play because the LPR system did not contain all the components and operations of a record keeping process. The court found the police department's passive use of the LPR system was legal.

Massachusetts Supreme Court
***Commonwealth of Massachusetts v. McCarthy*,**
484 Mass. 493, 142 N.E.3d 1090 (Mass. April 16, 2020).
https://law.justia.com/cases/massachusetts/supreme-court/2020/sjc-12750.html

Law enforcement officers were investigating Jason McCarthy's suspected illegal drug activity and deployed LPRs on bridges to track his activity. Police used data from the LPRs and received real-time alerts, which led to the arrest of McCarthy. McCarthy filed motion to suppress the LPR data because it violated his constitutional right to privacy of his public movements. The court ruled the defendant's privacy was not violated because of the limited extent and use of the LPR data.

Reasonable Suspicion for Vehicle Stop Based on License Plate Reader Information

---

United States Court of Appeals for the Ninth Circuit
***Denise Green v. City and County of San Francisco*,**
751 F.3d 1039 (9th Cir. 2014).
May 12, 2014
https://caselaw.findlaw.com/us-9th-circuit/1666208.html

An LPR operated by a San Francisco Police officer indicated a license plate displayed on Denise Green's vehicle was on a stolen vehicle. A high-risk felony stop occurred, and Green was held at gunpoint, handcuffed, and detained. Eventually, officers ran the actual plate to confirm stolen and determined the LPR misread the plate, and the vehicle was not stolen; Green was released.

San Francisco Police Department officers are trained that an LPR hit does not automatically justify a vehicle stop. Officers are directed to verify validity of the identified hit before executing a stop. Officers are instructed to verify the plate being read by the LPR is truly the plate on the vehicle and to confirm the stol-en "hit" with their police telecommunications system. **The court ruled an unconfirmed LPR "hit" does not form a reasonable suspicion to support an investigatory detention of subject.**

Georgia Court of Appeals
***Hernandez-Lopez v. The State of Georgia*,**
319 Ga. App. 662, 738 S.E.2d 116 (Ga. Ct. App. 2013).
February 5, 2013
https://caselaw.findlaw.com/ga-court-of-appeals/1622591.html

An LPR in use by an officer with the Gwinnett County, Georgia, Police Department indicated a plate belonged to a "wanted person" by the name of Eloy

Hernandez-Lopez. The officer noted a warrant was for an adult male, which matched the warrant identifying information. The vehicle was stopped and the subject operating the vehicle was determined to be Salomon Hernandez-Lopez, and he was arrested for operating without a license.

Hernandez-Lopez claimed the officer lacked reasonable suspicion to conduct a traffic stop based on the LPR information. The court held the officer did in fact have reasonable suspicion based on the LPR information indicating the license plate belonged to a "wanted person." This would be the same as if an officer ran the license plate through the Georgia police telecommunications system directly. **The court ruled an LPR "hit" provides an officer with reasonable suspicion to justify an investigatory stop.**

New York Supreme Court
***People of the State of New York v. Luis Davila, Jr.*, 27 Misc.3d 921, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. 2010), *aff'd*, 137 A.D.3d 655, 26 N.Y.S.3d 862 (N.Y. App. Div. 2016).**
April 1, 2010
https://law.justia.com/cases/new-york/other-courts/2010/2010-20111.html

A New York Police Department LPR mounted on a police vehicle alerted officers to a suspended plate, and the vehicle was stopped. An officer observed what appeared to be a weapon in possession of a vehicle occupant and subsequently arrested the subject for possession of a firearm. Davila contested the arrest, arguing the officer failed to follow department policy by first verifying the LPR data had been updated in the past 24 hours and did not verify the information against the department database. The court ruled the department policies are guidelines and not required by law; therefore, use of LPR to detect the vehicles registration as suspended was lawful.

Related Federal Statutes

28CFR Part 23 Criminal Intelligence Systems Operating Policies
28 CFR Part 23 contains policy standards for law enforcement agencies operating federally funded multijurisdictional criminal intelligence systems. The standards specifically provide guidance for the submission, entry, security, inquiry, dissemination, review, and purge of criminal intelligence information.

---

2 CFR § 200.79 Personally Identifiable Information (PII).
LPR information is NOT PII
PII is information considered capable of identifying an individual either by itself or with other identifying information. LPR systems contain information consisting of vehicle license plates, vehicle photos, dates, times, and GPS locations—information generally not considered PII. Therefore, LPR information may not be restricted by statutes concerning maintaining PII but can become PII if additional information is included that is defined as PII. Case-by-case assessment is recommended when developing LPR system data maintenance and use.

Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721
The Driver's Privacy Protection Act (DPPA), 18 U.S.C.A. §§ 2721-25 also supports the premise that a license plate number alone is not PII. Enacted in 1994, the DPPA is a federal law that regulates how state motor vehicle departments release information contained in their records. DPPA addresses the prohibition on release and use of certain personal information from state motor vehicle records. Collected LPR information contains no PII that may be used to connect a license plate detection to an individual. It is only with permissible purpose law enforcement may make this connection (using motor vehicle records).

Appendix B Additional License Plate Reader Resources

American Association of Motor Vehicles (AAMVA)

AAMVA – Best Practices and Model Legislation

- License Plate Standard, Edition 2 (2020)

AAMVA – AAMVA Policy Positions

- Alternative License Plates Policy Statement (Adopted 2020)
- License Plates Policy Statement (Amended 2020)
- License Plates Should Not Be Obscured Policy Statement (Amended 2020)
- Temporary License Plates Policy Statement (Amended 2020)

International Association of Chiefs of Police (IACP)

You must be an IACP member with log-in credentials to access these resources:

https://www.theiacp.org/resources/policy-center-resource/license-plate-readers

- IACP License Plate Reader Model Policy (2010)
- IACP License Plate Reader Concepts and Issues Paper (2010)

These IACP resources are publicly accessible:

https://www.theiacp.org/projects/automated-license-plate-recognition

- IACP License Plate Reader Privacy Impact Assessment (2009)
- IACP License Plate Reader Policy & Operational Guidance (2012)
- IACP Resolution: Retro-Reflective Front and Rear Plates (2018)
- IACP Resolution: Digital License Plates (2020)
- IACP Technology Policy Framework (2014)

Police Executive Research Forum

Free Online Documents (policeforum.org)

- Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology: Police Executive Research Forum, December 2011

RAND Corporation

https://www.rand.org/pubs/research_reports/RR467.html

- License Plate Readers for Law Enforcement – Opportunities and Obstacles (2014)

Appendix C Sample License Plate Reader Policies

Introduction

The core business values that License Plate Reader (LPR) promises can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all tools and technologies available to law enforcement, LPR must also be carefully managed. Agencies must clearly articulate their strategic goals and tactical objectives for the technology, and this strategy should be tightly aligned with the broader strategic plans of the agency. Thorough and ongoing training is required to ensure that the technology performs effectively and that users are well versed in the operational policies and procedures defined and enforced by the agency.

Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system and reassure the public that their privacy interests are recognized and respected.[1]

Three agency sample policies follow:

Ohio State Highway Patrol

Utah Tax Commission, Motor Vehicle Enforcement Division

Virginia State Police

1 IACP ALPR Policy & Operational Guidance (see Appendix B).

OHIO STATE HIGHWAY PATROL POLICY

Summary of Revisions

Revisions are in red, bold, italics throughout.

Purpose

To provide guidelines for the implementation, installation, and use of mobile and stationary Automatic Plate Reader (APR) technology and equipment at selected locations to scan, detect, and identify license plate numbers appears on selected "Hot Lists."

Policy

A. **STATEMENT OF POLICY –** The Ohio State Highway Patrol will utilize APR technology in patrol cars and at stationary locations to accurately identify license plates ***linked to criminal activity and/or commercial motor vehicle administrative violations.***

B. **FUNCTIONALITY AND OPERATION <41.3.9a>**

1. **Installation –** Stationary and mobile scanners will be installed at selected locations and on selected marked and unmarked vehicles. ***GHQ electronic technicians are responsible for maintaining a list of all locations and vehicles equipped with APR technology.***

2. Data Sources for "hits" – All APRs have the ability to match a captured image to two categories of databases: criminal violations and commercial motor vehicle violations. Officers and MCEIs have the ability to match images with one or both types of databases simultaneously.

a. Criminal Databases: Both mobile and stationary APRs can match captured images with LEADS and NCIC entries with an associated license plate (e.g., stolen motor vehicles, felony warrants, missing persons, protection orders, etc.)

b. Commercial Motor Vehicles – Both mobile and stationary APRs can match captured images with the Federal Motor Carrier Safety Administration PRISM database for commercial motor vehicles placed out of service and ones with an "Inspect" or "Possible" score in the Inspection Selection System (ISS).

3. General Operation – The Division's automatic plate readers capture images of numbers and letters resembling license plates and match those captured images to the current "hot list." The "hot list" is the master index of license plates entered in both data sources listed above. The criminal database "hot list" is updated twice daily and the commercial motor vehicle database "hot list" is updated once daily.

4. Units assigned to enforcement vehicles equipped with mobile APR systems shall ***verify the receipt of*** the most recent "Hot List" from the applicable databases at the beginning of each shift.

5. **Probable Cause** – An APR "hit" from the criminal databases shall not be used as probable cause for a traffic stop or enforcement contact. Contact with the vehicle and occupants shall only be made after the "hit" is confirmed through LEADS/NCIC.

6. **Manual Entry by User into "Hot List" Database** – ***The system does not obtain real***

time information from LEADS/NCIC; therefore, there may be situations which require an officer or dispatcher to manually enter a vehicle registration into the database. These situations include, but are not limited to: active Amber Alerts, Ohio Blue Alerts, endangered missing child alerts, endangered missing adult alerts, BOLOs, and other emergency messages/alerts. Manual entry of a plate into the "Hot List" shall only be done with supervisor approval. See User Manual for entry procedures.

A "hit" on a BOLO that is manually-entered into the system shall not be used as probable cause for a traffic stop or enforcement contact.

7. **'O' vs. Zero** – Because of standardized NCIC formats, a letter 'O' and a zero in a license plate number are synonymous in NCIC records. Therefore, the "hot list," NCIC, and the APR read the letter 'O' as a zero. Any plate entry, including any manually entered by an officer or a dispatcher with an 'O' is automatically converted to a zero.

8. **Fixed Point and APR Notification** – When a license plate entered in the "Hot List" is detected by a stationary APR, a notification is automatically sent by the APR system to an OSP dispatch facility equipped to receive the notifications. When a mobile APR detects a "Hot List" entry, the officer receives an audible and visual notification on the in-car MCT.

9. **Case Documentation** – A record of the APR "hit" shall be included in the case/incident report. All "hits" captured by the APR system shall be stored for 30 days and will then be automatically purged. All "hits" will be stored electronically in the ELSAG system. Access to the ELSAG system is limited to authorized personnel only. <41.3.9b,d>

10. **Storage of "Non-Hits"** – All "non-hit" APR captures shall be automatically purged from the system within a 24-hour period. APR captures shall not be collected, stored, or shared with the intent of data mining. Dispatchers assigned to Cleveland and the Statehouse shall query the system for plates older than 24-hours on a quarterly basis to ensure "non-hit" captures are being deleted in accordance with this policy. Troopers assigned APR equipped enforcement vehicles shall perform the same query as part of the semi-annual vehicle inspection. <41.3.9d>

11. **Training –** Dispatchers, sworn officers, electronic technicians, motor carrier enforcement inspectors, and network administrators shall receive appropriate training from qualified OSP staff or vendor representatives prior to using or maintaining the APR equipment. <41.3.9c>

C. **USER MANUALS –** The manufacturer's user manuals, which provide operational procedures for both the Mobile Auto-Detector User and Operations Center Personnel are attached to this policy.

D. **GUIDELINES FOR USE <41.3.9a>**

1. **Stationary APRs**

   a. **Notification** – After receiving a "hit" through LEADS/NCIC, the dispatcher will verify the APR "hit" on the plate matches the image and follow established procedures to check NCIC/LEADS. The dispatcher will then dispatch an officer to intercept the vehicle. Two officers will be dispatched to verify "hits" at the Statehouse Garage. The officer(s) will be notified of the reason for the "hit," that the dispatch is a result of the APR and that the "hit" has been verified through NCIC.

   b. **Verification of Hit** – If, for any reason, the APR "hit" cannot be verified through LEADS/NCIC, the vehicle is not to be stopped based solely on the APR. If the

Ohio State Highway Patrol Policy (continued)

dispatcher cannot read the digital image sufficiently to verify the license plate number and state, an officer may be dispatched to intercept the vehicle, however the intercepting officer must first verify the "hit" through NCIC prior to stopping the vehicle.

c. **Turnpike Gate Personnel** – If an officer is unavailable to immediately intercept a valid "hit," the dispatcher may notify additional personnel to be on the lookout for the suspect vehicle. Ability to identify the vehicle, reason for the "hit," and known direction of travel should all be used to determine whether additional personnel should be notified. If the vehicle is observed, they should be instructed to notify the dispatch facility of the route and direction of travel.

d. Officers and dispatchers should use their discretion based on hazards, proximity of assisting officers, type of "hit," etc.

e. **Cleveland Dispatch Center / Capitol Square Parking Facility**

i. The APR system will be checked by the dispatcher at the beginning of the shift and the information will be logged on the OTIS HP-53 using File 1 – Sub Category "APR."

ii. The Statistical Analysis function will determine if the APR is functioning correctly. The system should indicate a number of plates that have been checked. If there are no plates indicated, the system is not functioning. If the system shows that plates are being scanned, the system is working correctly.

iii. The Statistical Analysis section is found in section 6 of the User's Guide.

2. ***Mobile APRs***

a. Mobile APRs are operational as long as the officer is logged in to the MCT in the vehicle.

b. Officers have the ability to toggle between the Criminal and Commercial databases or they can activate both. If both databases are active, the mobile APR will indicate a "hit" on a violation in either system.

c. Officers must verify the "hit" through LEADS/NCIC prior to stopping the vehicle. If, for any reason, the APR "hit" cannot be verified, the vehicle is not to be stopped based solely on the APR. Officers only need to verify that the plate matches the "hit" in the FMCSA database.

d. Officers and MCEIs should use their discretion based on hazards, proximity of assisting officers, type of "hit," etc.

e. Motor Carrier Enforcement Inspectors may not stop a commercial motor vehicle for the sole purpose of a LEADS/NCIC "hit".

3. **Infrastructure Specialist and Electronic Technicians are responsible for:** <41.3.9b>

a. Equipment and software deployment and installation

b. Coordinating maintenance and repair

c. Coordinating the establishment of parameters for download of NCIC and LEADS

Ohio State Highway Patrol Policy (continued)

data, pick-up radius restrictions, misdemeanor and/or felony warrants.

d. Ensure all captures on stationary and mobile APRs follow the appropriate retention schedule.

4. **Public Affairs -** All media contacts will be coordinated through the Public Affairs Unit, which shall be consulted prior to releasing any information to the news media.

5. **Licensing and Commercial Standards**

   a. LCS units may stop commercial motor vehicles for the purpose of inspection based on hits received from the PRISM file "Hot List."

   b. The reason code LPRI (License Plate Reader Inspection) will be used in ASPEN for all inspections conducted based on a PRISM hit.

UTAH MVED POLICY

Policy
410

Utah Motor Vehicle Enforcement Division
Po icy Manua

Automated License Plate Readers (ALPRs)

410.1 PURPOSE AND SCOPE

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an “informational data file” containing information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle “hit” by an audible alert and an associated notation on the user’s computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras are transmitted to an ALPR server. The ALPR server resides within the State of Utah Data Network Center. In addition to software applications that are used to run the ALPR server, the ALPR server also houses the “informational data file” containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle File (SVF), “HOT FILE” (HF), Wanted Persons File (WPF), Stolen Plate File (SPF), Revoked Registration File (RRF), Cancelled Registration File (CRF), Expired Registration File (ERF), Out of Service (OS), and user defined “hot lists.“ The Informational data file is updated throughout the day with different data sources being “refreshed” at different intervals. SVF/WPF/SPF/RRF/ERF/OS data is refreshed from the state database daily, HF data is refreshed from the Bureau of Criminal Investigation hourly, CRF data is refreshed weekly, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database. When possible, confirm that the mobile ALPR unit hit information is still valid, either through your Communication Center (CC) or via your laptop computer (LC) prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if CC is contacted, it could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server as the scans occur. ALPR scans can be compared against the informational data file immediately when the data sources are updated. Mobile ALPR units do not have a continuous connection to the ALPR server. In order to facilitate the exchange of data, air cards are used which will allow connectivity to the ALPR server via wireless transmission.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah Motor Vehicle Enforcement Division

Po icy Manua

Automated License Plate Readers (ALPRs)

If the air card in the vehicle is connected to a service, the ALPR will continually “sync” which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at least once at the beginning of their shift to ensure they have the latest informational data available.

410.2 POLICY AND PROCEDURES

Mobile ALPR unit users receiving an alert shall confirm the status of the vehicle by running the license plate either manually via the LC or over the radio via CC, unless compelling circumstances are present or officer safety issues make it unsafe to do so.In such cases, Officers shall confirm the status of the alert as soon as possible. When requesting CC to confirm the status of an ALPR alert, the officer shall advise CC the request is for an ALPR alert.

In the case of a stolen vehicle alert, personnel may regard the vehicle as a known stolen vehicle, while awaiting a secondary confirmation. If the decision is made to initiate a “felony stop” due to an ALPR alert on a stolen vehicle, officers shall advise CC they are following a vehicle due to an ALPR stolen vehicle alert prior to receiving a secondary confirmation by LC/CC.

Officers shall adhere to the Department’s pursuit policy as described in the Manual of Policy and Procedures. CC shall immediately provide secondary confirmation or advise the unit that the vehicle is not reported as stolen.

When Desk Personnel receive an alert from a fixed ALPR system, which is the result of an image taken from a fixed camera, they shall confirm the current status of the vehicle via their CAD terminal or via CC. While waiting for confirmation, desk personnel will advise field patrol units of the ALPR alert, the location, the vehicle description, request aero bureau, and coordinate responding field units.

410.2.1 HOT LISTS

Hot lists are comprised of user defined data that is manually input into the informational data file so that ALPR users will be alerted whenever a “vehicle of interest” is located.Hot lists can be loaded into a specific station area vehicle or to ALPR all vehicles countywide.

Hot lists can be input into the ALPR server informational data file only by ALPR administrators. Unit commanders, or their designees, must approve hot list information that is intended for use solely in their area cars. With the exception of AMBER alert information, hot list information intended for Department-wide use must have the approval of the Division Director, or his designee.Mobile ALPR users can input individual license plates into their patrol vehicle’s ALPR system for use during their shift, however, the information will be deleted from that mobile ALPR unit once user performs an “end shift” and the vehicle syncs with the ALPR server. An ALPR vehicle alert identified via hot list information does not automatically provide ALPR users with sufficient justification to pullover or detain vehicle occupants. Often times, these hotlists will identify a “vehicle of interest” which is not necessarily wanted for a crime (ex: sex offender vehicle).

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah MVED Policy (continued)

Personnel must use discretion and in some cases have independent information justifying a traffic stop.

410.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official and legitimate law enforcement business (Utah Code 41-6a-2003).

(b) An ALPR may be used in conjunction with any routine patrol operation or official investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) If practicable, the investigator should verify an ALPR response through the Utah Department of Public Safety (DPS) law enforcement information system or other appropriate database before taking enforcement action that is based solely upon an ALPR alert.

(f) No ALPR operator may access the DPS database or other system unless otherwise authorized to do so.

410.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Utah Motor Vehicle Enforcement Division and because such data may contain confidential information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law (Utah Code 41-6a-2004).

The Administration Lieutenant is responsible to ensure proper collection and retention of ALPR data, and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

All ALPR data downloaded to the server should be stored for the minimum period established by department records retention guidelines and thereafter should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action. In no event shall data be maintained longer than nine months unless it is subject to a warrant, preservation request or disclosure order (Utah Code 41-6a-2004). Data that will not be purged should be downloaded from the server onto portable media and booked into evidence.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Utah Motor Vehicle Enforcement Division
Po icy Manua

Automated License Plate Readers (ALPRs)

410.4.1 NON-GOVERNMENTAL AGENCY ALPR
ALPR data captured by a non-governmental agency device may only be obtained pursuant to a warrant or a court order (Utah Code 41-6a-2005).

410.5 ACCOUNTABILITY AND SAFEGUARDS
All saved data will be closely safeguarded and protected by both procedural and technological means. The Utah Motor Vehicle Enforcement Division will observe the following safeguards regarding access to and use of stored data:

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Office Manager and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(e) ALPR system audits should be conducted on a regular basis.

Copyright Lexipol, LLC 2020/08/26, All Rights Reserved.
Published with permission by Utah Motor Vehicle Enforcement Division

Virginia State Police Policy

Virginia Department of State Police

General Order OPR 1.20 **License Plate Reader Operating Procedures**

Purpose: To establish uniform guidelines for License Plate Reader operations by Department personnel.

1. The License Plate Reader (LPR) program is intended to enhance law enforcement operations related to homeland security and terrorist watch lists, stolen vehicles and license plates, sex offender violators, wanted and missing persons, and other vehicle-related crimes that impact the safety of citizens.

2. The Director of the Bureau of Field Operations (BFO) shall appoint a Statewide LPR Program Coordinator who shall be responsible for the daily operations of the LPR Program.

Guidelines for Use

3. The Department's LPR system shall be used for official law enforcement purposes only. No employee may use, or authorize the use of, the equipment or database records for any other reason. Misuse of equipment or database records may result in disciplinary action.

4. LPR units will be installed in Department vehicles as determined by the Director of BFO or his/her designee. The Director of BFO must pre-approve the transfer of an LPR unit to another Area. Otherwise, if a sworn employee assigned a vehicle equipped with an LPR unit is transferred, promoted or resigns, the vehicle will be reassigned to another sworn employee and retained in the original Area.

5. LPR-equipped vehicles may be used for routine patrol or during special events. In all instances, LPR-equipped vehicles shall be operated in accordance with Department policies regarding vehicle operations.

6. Each employee assigned an LPR unit is responsible for ensuring they are operating with the most current "Hotlist" at the beginning of each shift. The Statewide LPR Program Coordinator should be contacted immediately if problems are encountered with the updating of the LPR units.

7. Upon receiving an alarm or hit, the sworn employee shall verify the accuracy of the information by contacting the Communications Center per established Department policy.

Effective Date – 10/1/2018 Review Date – 7/1/2022
BFO

General Order OPR 1.20

a. An LPR alarm alone is NOT sufficient probable cause to warrant a stop or arrest.

b. Sworn employees are required to confirm a positive hit prior to any enforcement action being taken.

8. Sworn employees are required to ensure that all positive hits on the Terrorist Watch List are reported to the Terrorist Screening Center (TSC) and Virginia Fusion Center (VFC) immediately. All Terrorist Watch List hits will be handled by MDT or telephone. There will be no radio traffic concerning terrorist hits except in the case of emergencies.

9. Special circumstances, such as AMBER Alerts or critical incidents, may require immediate manual updating of the LPR system "hot list." Sworn employees in possession of license plate information related to such circumstances will immediately enter the data into the LPR system. The Virginia Fusion Center (between 0600 and 2200 hours) and/or Statewide LPR Program Coordinator will ensure that new information is uploaded or relayed to all active LPR units. If a critical situation requires manual entry of license plate data, the Communications Center shall immediately notify all LPR users of the new data in the Division and document this action in the CAD system. LPR users shall manually enter the license plate information associated with the critical incident. The Communications Center shall also contact the Virginia Fusion Center and provide the information so that the data may be entered into the statewide list.

10. Terrorist organizations have openly voiced their desire to attack venues where large crowds gather, such as major sporting events, large festivals, etc. Because of the potential of just such an incident, stationary, mobile, and covert LPR use is permitted for such events. Prior to utilizing LPRs at these venues, the affected Division Commander shall submit a letter, through channels, to the Superintendent describing the event, potential threat, and parameters under which the LPRs will be utilized. The decision to grant the approval rests with the Superintendent's Office.

11. Fixed and/or covert LPR units may be used to support on-going criminal investigations or approved venues. The use of fixed and/or covert LPR units shall be coordinated with the Statewide LPR Program Coordinator.

12. At the end of each month, Monthly Plate Reader Activity Logs will be submitted to the appropriate Area Office and Division LPR Coordinator by personnel using an LPR unit.

General Order OPR 1.20

a. At the Area office, a separate file will be maintained for each LPR unit assigned to the Area. Each file will include all Monthly Plate Reader Activity Logs submitted after LPR system usage. These logs will be handled as Department-governed non-records (DGNRs) and shall be retained for two years after the end of the calendar year.

b. At the Division headquarters, all Monthly Plate Reader Activity Logs will be reviewed by the Division LPR Coordinator and consolidated into one Monthly Plate Reader Activity Report. The report shall be reviewed by the Division Commander and forwarded to the Statewide LPR Program Coordinator by the 5th of each month. The Division is the record holder for the Monthly Plate Reader Activity Reports, and these reports shall be included on the Division's file list. Monthly Plate Reader Activity Reports shall be retained for two years after the end of the calendar year.

Data Security and Access

13. The Statewide LPR Program Coordinator is responsible for overall operations of the program, including:

    a. controlling access of sworn personnel to the LPR system and hot file data;

    b. ensuring stored data are purged from the LPR system server as required;

    c. approving or denying in writing requests to access and/or use LPR data; and,

    d. designating personnel who will be authorized to access the server and conduct data queries.

14. The Department's Data Center will house the Department's LPR System Operations Center, which is the central database for all license plates scanned by the Department's LPR units.

    a. All collected data will be maintained on an independent server that is not connected to, or shared with, other law enforcement databases.

    b. The Data Center will provide an inquiry tool, history tracking, and reporting protocols for the entire LPR program.

    c. The Data Center will provide a secure intranet site, allowing only approved personnel password-protected access to collected data. This access shall be restricted to:

General Order OPR 1.20

(1) searching for a license plate or partial license plate;

(2) viewing the image and location of matches on the "hot list";

(3) viewing maps showing the location of alarms or hits;

(4) viewing statistical reports on alarms or hits; and,

(5) searching for matches for a specific geographical location and/or time frame.

Operator Training

15. All users must receive standardized training prior to operating the LPR system.

a. The Statewide LPR Program Coordinator is responsible for providing initial training of all Department personnel who utilize the LPR system.

b. Additional training will be provided as needed and as determined by the Statewide LPR Program Coordinator.

c. The Training Division will be responsible for maintaining and updated all training records associated with the LPR program.

Data Storage and Retention

16. Per the Virginia Attorney General's Opinion #12-073, "License Plate Readers – Use and Storage of Data," the Department may not passively collect and store plate read data for potential use in future investigations.

a. The collection and use of stored data to help solve future crime are prohibited under the Opinion and existing Virginia law.

b. The Department may continue to use the LPRs to compare active reads to existing lists, such as stolen vehicles or Amber Alerts. Only the reads that are directly related to the intended purpose (i.e., stolen plate) may be retained beyond the use session of the LPR. All other non-relevant, passive reads should be deleted at the end of that day's use.

c. The Department may collect, store, and analyze data that relates to a specific, on-going, active investigation. That data shall be made part of the criminal investigative file and may not be used for other purposes.

General Order OPR 1.20

d. The Department may collect and temporarily store data that relates to special events as enumerated in paragraphs 10 and 11 of this General Order. This data will only be stored during the event and will be disposed of immediately following the event if it has been determined no applicable criminal investigation has been initiated. If an applicable criminal investigation is initiated, the data will be handled in accordance with paragraph 16.c. of this General Order.

Appendix D AAMVA License Plate Reader Working Group Roster

CHAIR AND LAW ENFORCEMENT REPRESENTATIVE

Captain Matthew Beaudin
Colorado State Patrol

LAW ENFORCEMENT REPRESENTATIVES

First Sergeant Robert Alessi
Virginia State Police

Lieutenant Chris LaPrairie
Nevada Highway Patrol

Captain Joseph Moody
North Carolina Department of Motor Vehicles
License & Theft Bureau

Colonel Allan Shinney
Utah State Tax Commission

Sergeant Jonathan Zarkauskas
Virginia State Police

MVA REPRESENTATIVES

Betty Johnson
Division Administrator
Nebraska Department of Motor Vehicles

Rosa Yaeger
Director
South Dakota Department of Revenue

IACP REPRESENTATIVE (MEMBER)

Major Josh Swindell
Ohio State Highway Patrol

IACP REPRESENTATIVE (STAFF)

Ryan Daugirda
International Association of Chiefs of Police

TECHNICAL ADVISORS

Dennis Bernardo D'Annunzio
Firmware and Software Development Manager
Leonardo

Jeff Hielsberg
Regional Sales Director
Intellectual Technology, Inc.

Kyle Hoertsch
Vice President of Public Safety Client Relations
Motorola Solutions

Steve Vaughn
Vice President of Field Operations
PrePass Safety Alliance

Mark Muriello
Director, Policy & Government Affairs
International Bridge, Tunnel and Turnpike Association

AAMVA STAFF – PROJECT MANAGER

Brian Ursino
Director, Law Enforcement Programs
American Association of Motor Vehicle Administrators

AAMVA STAFF

Paul Steier
Director, Vehicle Programs
American Association of Motor Vehicle Administrators

MSP- ALPR Private Network Options

March 1st, 2021

verizon

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Mobile Private Network via IPSec VPN to AWS

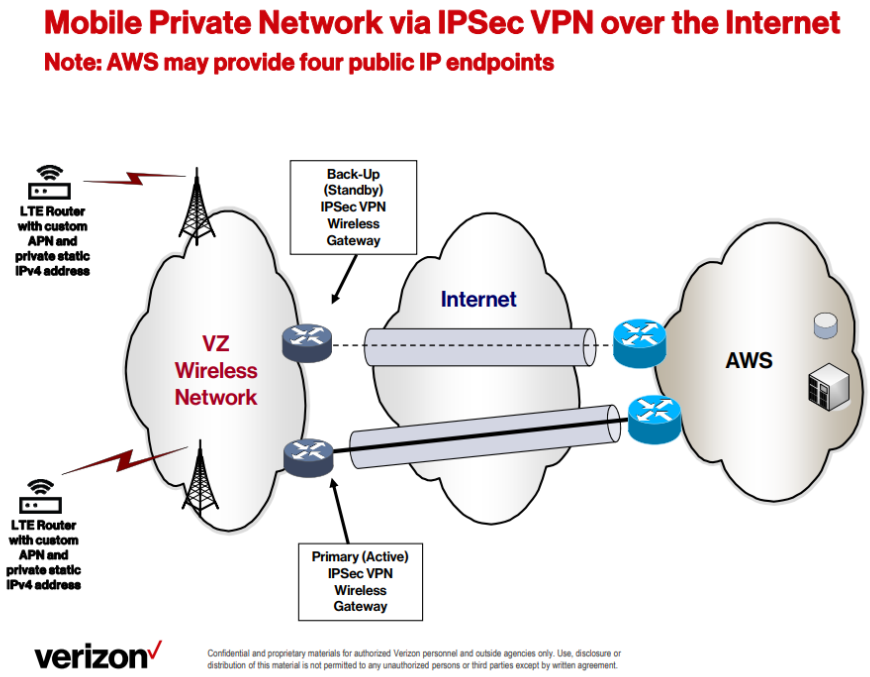
Project goals- enable remote access to ALPR modems. Simplify management

Brief Operations/ Account Set up Description:

- Separate APN for this network
- Private network with “MSP” as the parent and any other organizations that MSP authorizes would be “child accounts”- with cameras sending data to AWS and mobiles billed to the agency/municipality separately as they are today .
- Wireless Enterprise Help Desk- Tier 3 7 x 24 help desk available only to authorized customers (MSP is one) and private network customers (child accounts would also have access)

Costs: VZW Private network set up costs are waived for public safety customers under ITT72. MSP will continue to receive the same charges for the mobiles.

Other costs- MSP Pls confirm AWS Costs. These would be billed from AWS to the Commonwealth



Separate APN.

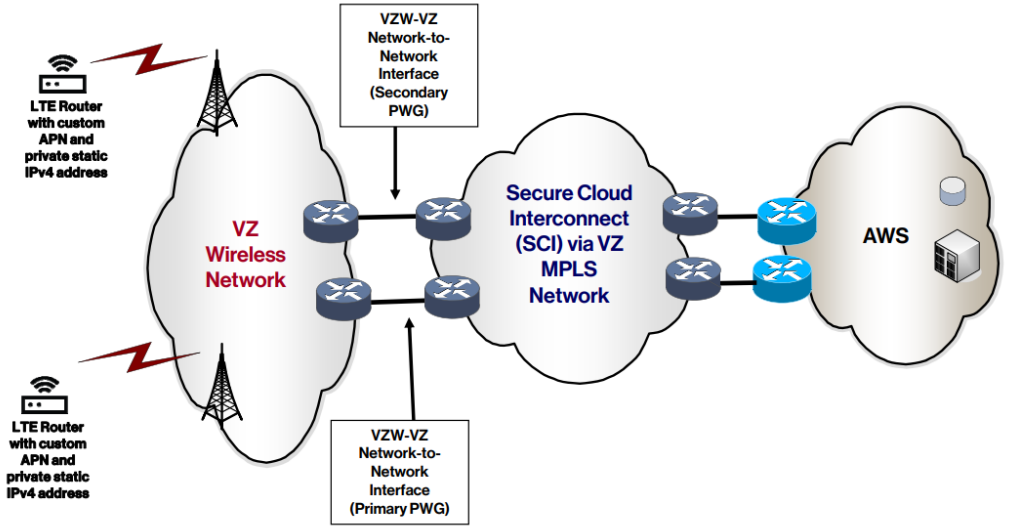
Mobile Private Network via Secure Cloud Interconnect

Project goals- enable remote access to ALPR modems.
Simplify management

Operations/ Account Quick Set up Description:

- Separate APN
- Traffic is not on the internet
- Customer provided private IP Addresses. MSP would assign subnets to parent/child devices
- Private network with “MSP” as the parent and any other organizations that MSP authorizes would be “child accounts”- with cameras sending data to AWS and mobiles billed to the agency/municipality separately as they are today
- Wireless Enterprise Help Desk- Tier 3 7 x 24 help desk available only to authorized customers (MSP is one) and private network customers (child accounts would also have access)

Mobile Private Network via Secure Cloud Interconnect
(SCI) Leveraging Private Wireless Gateway (PWG) and the VZ MPLS Network



Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Estimated SCI Pricing

The pricing below is an estimate based on the information we have currently. We wanted to display the cost items associated with this solution. Once we have a better understanding of the total throughput requirements we will be able to adjust this pricing to accurately represent the final solution.

10M Access (100M UNI) = $198.00 MRC

10M Private IP Port = $153.00 MRC

100M Wireless Gateway = $510.00 MRC

1,000GB SCI Plan = $500.00 MRC

Total Solution = $1,361.00 MRC

Wireless Costs- private network installation cost is waived for qualifying public safety customers (MSP is qualified). Mobile costs will continue to bill at the same rates.

verizon

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Home Office

National ANPR Standards for Policing and Law Enforcement

November 2020

Version: 2.1

1. Executive Summary

These standards articulate the requirements with which the police and other Law Enforcement Agencies (LEA), as detailed at Annex A must comply to access the National ANPR Capability (NAC). These standards do not cover the use of Automatic Number Plate Recognition (ANPR) for any purpose that is not law enforcement and will identify the purposes for which this document shall be applicable. Data from the NAC may not be used for other purposes, however in appropriate circumstances a camera may provide data to both the NAC and organisations other than those listed at Annex A to be managed independently.

This document includes a description of the legal basis for ANPR as well as the applicability of these standards. The standards comprise three main sections: Data Standards, Infrastructure Standards and Data Access and Management Standards. Audit standards and technical requirements are covered in other documents.

Data Standards comprise the security requirements that must be met for the NAC as well as the composition requirements for read data.

Infrastructure Standards cover the end-to-end infrastructure requirements for the NAC, including infrastructure development, cameras, networks, databases, infrastructure access and performance and legal requirements.

Data Access and Management Standards include the management of data within the NAC, including collection, storage, transfer and deletion of data. This section also provides guidance on FOI and Data Protection Act (DPA) enquiries.

The Annexes to this document include password requirements, guidance on investigation categories, the approval process for accessing ANPR data and a list of approved organisations that may access ANPR.

2. Contents

1. Executive Summary 2

Definitions 5

3. Introduction 8

4. Background 9

5. ANPR Legislation 10

6. Applicability 12

7. Part 1: Data Standards 13

7.1. Data Standards Overview 13

7.2. Data Security 13

8. Part 2: Infrastructure Standards 16

9. Part 3: Data Access and Management Standards 28

Annex A: Approved Organisations 38

Annex B: Investigation Categories 40

Major Investigations 40

Serious Investigations 41

Priority and Volume Investigations 43

Annex C: Data Access Requirements 45

Appendix A: Password Requirements 47

Document Revisions

Version 1.1 draft	July 2020	Change ref from CAST to DSTL in 8.14 Clarification at 9.8 re Command and Control Update of links within text
Version 2.0	September 2020	Published with amendments as above
Version 2.1	November 2020	Footnote added re data deletion (para 9.5.1)

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
Audit Standards	National Standards for Compliance and Audit of Law Enforcement ANPR
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CCA	Crime and Courts Act 2013
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
GSCP	Government Security Classifications Policy – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ICO Code	ICO Code of Practice for Surveillance Camera Systems

ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Arrangements under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC

NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information
PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
TSpec	The document prescribing the technical specifications for data within the National ANPR Service (NAS) to comply with the requirements of NASPLE.
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

3. Introduction

The Home Office issues these standards in support of the management and use of the National ANPR Service (NAS). ANPR is used by the police and other law enforcement agencies (hereafter referred to as LEAs) for law enforcement purposes. LEAs should use these policy standards to shape technical standards, standard operating procedures and audit standards.

This document covers the use of ANPR within the NAC and will identify for which uses this document shall be applicable. The use of ANPR within the NAC otherwise than in accordance with this document is not permitted.

This document is divided into 3 sections:

- Part 1 – Data Standards, which define the compliance requirements for ANPR Data
- Part 2 – Infrastructure Standards, which define the compliance requirements for ANPR infrastructure
- Part 3 – Data Access and Management Standards, which define the access requirements for LEAs and other organisations that are associated with ANPR data for law enforcement purposes.

4. Background

ANPR technology is used to help detect, deter and disrupt criminality at a local, force, regional and national level. This includes tackling traveling criminals, Organised Crime Groups and terrorists. ANPR provides lines of enquiry and evidence in the investigation of crime and is used by LEAs throughout England, Wales, Scotland and Northern Ireland.

There exists a National Law Enforcement ANPR capability (NAC) which enables LEAs to benefit from operational use of ANPR. The NAC comprises:

- The NAS. This is a single national system comprising standardised functionality to enable use for operational response, investigation and intelligence purposes as well as a single national store of data;
- The National ANPR Infrastructure (NAI), which is a network of ANPR cameras, communications links, firewalls and other related supporting components. Any element of this network that is connected to the NAS shall be the responsibility of the LEA that manages that connection.

4.1 Technical Specifications

Technical specifications for the NAC are detailed within a technical specification document (TSpec). LEAs are required to conform to the requirements of that document.

5. ANPR Legislation

ANPR operates under a complex framework of legislation of general application, including the General Data Protection Regulation (GDPR), the DPA, the Surveillance Camera Code and Common Law.

The National Law Enforcement ANPR capability (NAC) is subject to the Information Commissioner's Office regulatory provisions and regulatory oversight by the Surveillance Camera Commissioner (SCC).[1]

5.1. ANPR Data: Legal Basis

ANPR data from police forces is police information within the meaning of The Code of Practice on the Management of Police Information 2005 (MoPI) made under the Police Act 1996 and Police Act 1997. It may be shared between LEAs in accordance with the provisions of that Code or any other document which applies similar standards in its place, including the National Crime Agency's (NCA) Statement of Information Management Practice (SIMP).

Access to and the retention and management of ANPR data obtained by LEAs must be compatible and consistent with their relevant legal obligations, which include: The Data Protection Legislation (i.e. the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA));

- ICO Code of Practice for Surveillance Camera Systems (ICO Code);
- College of Policing Approved Professional Practice – Information Management. (MOPI);
- Part 2 of the Protection of Freedoms Act 2012 (PoFA);
- The Surveillance Camera Code issued under Part 2 of PoFA.
- Criminal Procedure and Investigations Act 1996 and Code of Practice issued under Part II of that Act (CPIA);

[1] Section 29(6) of the PoFA includes ANPR as one of a number of surveillance camera systems under the regulatory oversight of the SCC and its associated Home Office code of practice. Relevant authorities (as defined by Section 33 (s33) of PoFA) in England and Wales (including the police) must have regard to the code which provides guidance on the appropriate and effective use of surveillance camera systems, and therefore ANPR

5.2. Use of ANPR for Law Enforcement Purposes

ANPR infrastructure may only be deployed law enforcement purposes as defined in Part 3 of the DPA ; or on grounds of national security. Law Enforcement is defined by the DPA as “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. The Joint Controller Arrangements (JCA).

The JCA details the responsibilities of controllers for compliance with the DPA. The National Police Chiefs’ Council (NPCC) ANPR lead is designated as the lead controller within the JCA for the NAS.

Joint Controllers have determined within the JCA that they will conform to consistent policy and procedures for the elements of the NAC for which their own LEA is responsible and for which they are controller.

5.3. ANPR Audit

The Home Office has also issued a separate document entitled “National Standards for Compliance and Audit of Law Enforcement ANPR” (Audit Standards). This document sets out the requirements for compliance and audit by all LEAs and of the national components of the NAC.

6. Applicability

These standards apply to any NAC operated by LEAs in the UK that connect to or receive data from the NAS.

Where, under an agreement, LEAs receive data from components that are under the ownership or control of other organisations it is the responsibility of the receiving LEA to ensure compliance with the NASPLE.

ANPR cameras that are used solely for speed enforcement are outside the scope of these standards.

ANPR systems that are not operated by LEAs and do not submit data to the NAS are similarly outside the scope of these standards.

6.1. Approved Organisations

An LEA may only connect to, or receive data from, the NAS following approval of the NPCC policing lead for ANPR within the NPCC Crime Operations Committee (NPCC policing lead for ANPR) - an "Approved Organisation".

For an organisation to be designated as an "Approved Organisation" it must be involved in and can lawfully process data for one or more of the following activities:

- National security and counter terrorism
- Law enforcement
    - The prevention and detection of crime
    - The apprehension and prosecution of offenders

In granting access, the NPCC policing lead for ANPR must be satisfied that it is necessary and proportionate for the organisation to be approved.

Approved Organisations must ensure that their organisation complies with the requirements of NASPLE and Compliance and Audit Standards.

References to LEAs within NASPLE includes only "Approved Organisations" unless indicated otherwise. Approved Organisations are listed in Annex A.

In addition to the above purposes LEAs may use the NAS for operational purposes relevant to individual and public safety. E.g Missing persons.

7. Part 1: Data Standards

7.1. Data Standards Overview

Part 1 prescribes the standards with which data must comply for it to be accepted into the NAS.

7.2. Data Security

LEAs have a duty to protect ANPR data to ensure its integrity and to maintain its value for law enforcement purposes. ANPR 'read' data must therefore be attributed a protective marking of OFFICIAL, in accordance with the Government Security Classifications Policy (GSCP).

When in the NAS database, other material could be accessed such that personal details of persons associated with the ANPR READ data may be identified. Once ANPR READ data is available within the NAS, it is personal data in the context of the DPA.

All ANPR data in the NAS, should therefore be managed in accordance with DPA principles and handled as OFFICIAL - SENSITIVE data, in accordance with the GSCP.

Whilst in the custody of, or being transmitted to or from a LEA, ANPR data should be handled in accordance with Part 2 and Part 3 of NASPLE.

Access to data within ANPR systems must be in accordance with Part 3 of NASPLE.

7.3. ANPR Read Records

7.3.1. Composition

An ANPR READ places a VRM at a specific location and time. It is obtained by a camera as part of an automatic number plate reading system. The data components of a record must not be entered manually into the NAS unless for the purposes of correcting a mis-read VRM on the system or by an administrator for testing the connectivity of a camera.

The READs must include VRM, time, location of read and camera identifier and be consistent with the requirements of section 7.4.

7.4. Core Data

7.4.1. Vehicle Registration Mark (Mandatory)

ANPR data must accurately represent VRMs of all vehicles with correctly represented EU and Schengen Community number plates. Systems must accurately record the VRM for vehicles passing within the field of view for each camera. The capture and read rates must be in accordance with the type of camera defined at Section 8.9.

7.4.2. Vehicle Registration Mark – Not Read (Mandatory where functionality is in place)

Where a CAMERA has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, information will be recorded in the VRM field in accordance with current TSpec.

7.4.3. Time (Mandatory)

System audit provisions must provide evidence of synchronisation at least once every 10 minutes using standard time source techniques in accordance with current TSpec.

Components of ANPR systems must automatically adjust the display of the time to daylight saving time during the period when this is in-force.

7.4.4. Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

7.4.5. Supporting Imagery

In order to assist with assessment of the accuracy of individual read records, ANPR data may include images:

- Plate patch – showing the number plate only, to allow comparison of the visual image with the textual representation interpreted (Mandatory for systems under ownership or control of a LEA)
- Overview Image – showing the vehicle to allow identification of the make, model and colour of the vehicle within the read zone (Optional)
- 'Geo Tagging' - if an accurate GPS Geo Location is available, then this detail may be added to images (Optional)

Should any image be found to exceed prescribed limits for image size, cameras submitting the images must be revised to ensure images obtained are within the limits prescribed within a maximum of 7 days.

All images must be linked to the corresponding read record.

All images recorded must be forwarded to the NAS. Where no overview image has been recorded, the read record must include a reference to identify that no image is recorded.

7.4.6. Record Retention and Deletion

All read records received by LEAs including any associated images must be supplied to the NAS.

All records must be managed and subsequently deleted in accordance Section 9.5.

7.4.7. Camera Performance Evaluation

Camera Performance evaluation, as detailed in Section 8.14 of all components within LEA ANPR systems must be conducted to ensure compliance with the Data Standards. Where performance falls below the Data Standards then this must be corrected and reassessed to confirm that performance conforms to data standards, within 30 days of that issue being identified.

If camera performance issues are not resolved within 30 days of identification, then the feed of data from those cameras must cease until corrected.

8. Part 2: Infrastructure Standards

8.1. Infrastructure Standards Overview

Part 2 prescribes the standards for the components of the NAC, including the operability standards required that are to be used by LEAs connected to the NAS.

8.2. Accreditation

To preserve the integrity of the NAC, all components of infrastructure that connect to the NAS must be assessed to ensure that they do not pose a threat to the NAC and are suitably for handling data up to GSC OFFICIAL level.

8.3. LEA Domain

The assessment of risk to an LEA domain rests with the controller for each LEA, which will normally be discharged by the Information Security Officer (ISO) for that LEA. The level of risk posed should be determined through completion of a Risk Analysis Document and an IT health check (ITHC). Review of compliance with the risk analysis outcomes and the conduct of an ITHC is to be completed annually.

8.4. ANPR Network

The National Accreditor for Police Systems (NAPS) needs to be assured that the local LEA Infrastructure poses no threat to NAC. The NAPS will liaise with the LEA ISO to assess the level of risk posed, as documented through the LEA corporate information risk management and ITHC process.

The NAPS will approve the components of local infrastructure for connection to the ANPR Network. This will be confirmed by the completion of the Code of Connection.

8.5. ANPR Infrastructure Development

A consistent and standardised approach must be applied to infrastructure development within the NAC.

8.5.1. Strategic Assessments

A strategic assessment should be carried out prior to the deployment of an ANPR camera. An assessment should also be carried out prior to receiving ANPR data for onward submission to the NAS, that is received from ANPR systems operated by organisations that are not defined as LEAs. These assessments must identify a need for ANPR at that location for law enforcement purposes.

Where a need is identified, consideration of whether the deployment, or the receipt of ANPR data is appropriate and proportionate. This requires an assessment of the

value for law enforcement purposes taking account of the impact on fundamental rights and freedoms of individuals. Consideration of the legitimate expectations of individual privacy is also required. Strategic assessment should consider:

- National Security and Counter Terrorism,
- Serious, Organised and Major Crime
- Local Crime,
- Community Confidence and Reassurance, Crime Prevention and Reduction.

8.5.2. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA), which may include consultations with relevant stakeholders, is required for all planned new infrastructure.

The DPIA must include:

- A description of the proposed development
- An assessment of the risks to the fundamental rights and freedoms of individuals – the data subjects.
- Measures to mitigate those risks
- Confirmation of safeguards and security measures to ensure protection of personal data and compliance with the DPA.
- Details of any stakeholder consultation

8.5.3. Information Commissioner's Office Consultation

The NAC may result in high risk to the rights and freedoms of individuals and prior consultation with the Information Commissioner's Office (ICO) may be required before the deployment of any new ANPR infrastructure. When a DPIA identifies a large increase in the number of deployed ANPR infrastructure or where significant privacy risks are identified the ICO should be consulted. (Section 64 DPA)

8.5.4. Strategic Assessment Reviews

LEAs must monitor the continued requirement for a camera to be maintained at a location, or for an LEA to receive data from ANPR systems operated by other organisations. Should the justification for deployment at that location cease, the device must be removed, and the receipt of data must be terminated.

The locations of all cameras and the need to receive data from systems operated by other organisations must be reviewed annually, considering requirements for infrastructure development to ensure that camera deployment or receipt of data remains appropriate and proportionate.

8.6. Vehicle-Mounted Systems

Vehicle-mounted ANPR may only be deployed where any of the following circumstances arise:

- For the purposes of monitoring hits against a list of VOI with the intention that an operational response to the hit will take place, either by staff within the vehicle containing the ANPR system or by others deployed in support of that vehicle for the purpose of providing a response.
- Deployed at locations identified following completion of infrastructure development assessment prior to the deployment of other camera at the location.
- Deployed as a result of Operational tasking processes within an LEA where it has been determined that it is proportionate for short-term deployment of ANPR;
    - In response to identified criminal activity
    - In response to identified community problems
- To support assessment of a location for future more permanent camera deployment in accordance with the infrastructure development procedure
- In support of immediate operational response following report of a crime or incident.

8.7. System Standards

The performance standards for camera shown below are most easily met for vehicles travelling towards a camera, and it is recommended that unless unavoidable, for example in some dual-lane deployments, that this configuration is used in all cases.

8.7.1. Static ANPR Systems

A static ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs and is located in a fixed position, with no intention of the system being moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye[2] and accurately read 95% of captured VRM.

8.7.2. Moveable ANPR Systems

A moveable ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs, is located in a fixed position on a temporary basis and may be

[2] 'Visible to the Human eye' should be determined from the viewpoint of the camera within the ANPR system. A number plate visible to a 'human eye' at that location should also be visible by the ANPR system.

moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.3. Multi-Lane ANPR Systems

A Multi-Lane ANPR system has the capability to read VRM for vehicles travelling in multiple lanes of the highway using a single camera. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. For vehicles travelling towards the camera, systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

For vehicles travelling away from the camera, the system must capture 90% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.4. CCTV Integrated ANPR Systems

A CCTV Integrated ANPR system may operate both as a CCTV camera and as an ANPR camera. The camera should be optimised[3] for the purposes of ANPR when being deployed as a camera. Integrated systems must only provide data to the NAS when in ANPR mode. Except in extreme weather conditions the performance standards for these systems must be achieved at all times when deployed in ANPR mode. CCTV systems may not be optimised to capture ANPR reads therefore systems must capture 85% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.5. Mobile ANPR Systems

A mobile ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs. These include vehicle-mounted ANPR systems and other portable systems deployed on a temporary basis. Any equipment procured after the publication of version 1 of National ANPR Standards for Policing (NASP) (May 2013) must be live-linked to the NAS.

To achieve the optimum performance requirements, mobile equipment should be capable of night-time and low-light operation. Except in extreme weather conditions the performance standards for these systems must be achieved at all times.

Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM unless deployed in a moving vehicle, when the system must capture 80% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

[3] The optimum configuration of CCTV systems differs when used for general CCTV surveillance to when operated as an ANPR reader. It needs to be configured for ANPR use to ensure maximum possible data accuracy

8.7.6. Covert Systems

It is recognised that circumstances may arise where moveable or purpose-built, covert systems are deployed in support of an investigation in circumstances where it is not possible to establish a live-link to the NAS. Deployments of this type that are authorised within provisions of the RIPA or RIPSA are the only circumstances where equipment procured after the publication of version 1 of NASP (May 2013) may not have the capability to live-link to the NAS.

Unless unachievable due the nature of the deployment or in extreme weather conditions, the performance standards for these systems must be achieved at all times. Systems must capture 98% of al VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.8. Camera Access Settings

Unless a camera is designated a 'Restricted Access' camera, all cameras that submit data to NAS must be attributed the settings of 'Open Access', such that all data received from that camera is visible to all users with appropriate permissions to access the data.

With appropriate authority, a camera may be designated a 'Restricted Access' camera. Designation of a camera for 'Restricted Access' may only be authorised by a senior manager. A 'Restricted Access' camera may or may not be covert and the designation of a device for 'Restricted Access' may require authorisation within the provisions of the RIPA or RIPSA.

A record of all authorisations for restricted access must be retained for the duration of the restriction and a period of 2 years thereafter.

8.9. System Capability and Resilience

8.9.1. Image Capture

All cameras under the ownership or control of LEAs must have the capability to capture and record supporting imagery in accordance with section 7.4.5.

There may be circumstances where the shared collection equipment that is owned and managed by a non-LEA organisation is being used that are not enabled for the recording of imagery. In these circumstance, these cameras may be connected to the NAS subject to the standards for ANPR Infrastructure Development.

Supporting Images are important to assist with the accuracy of individual capture records and therefore, where data is received from other a non-LEA organisation without supporting images, provision for upgrading of the system to enable the provision of images should be established.

8.9.2. Schengen Information Systems (SIS)

All ANPR systems must be capable of reading plates that form part of the SCHENGEN community.

8.9.3. Data Storage

The NAS must not allow any data loss.

8.9.4. Local System Resilience

All local ANPR systems must transfer data to the NAS on receipt in local systems from a camera and also have the capacity to retain ANPR reads and their related images for a minimum of 3 and a maximum of 7 days from the time of the ANPR read.

This will provide resilience should the local infrastructure connections, the NAS or communications to the NAS become unavailable and will prevent the loss of data. In the event of a failure to send read records and associated images to the NAS local systems must have the capability to re-send that data.

If for any reason reads from a camera are submitted to the local system more than 7 days after initial capture the reads may be retained on the local system for 24 hours to prevent loss of data, should connection to the NAS become unavailable.

8.9.5. Local system connection and data transfer

Local ANPR systems must not enable connection to or the transfer of data to ANPR systems operated by other LEA for the purposes of searching of data or monitoring of VOI lists.

During the period of any loss of connection to NAS local functionality may provide for basic search of a full or partial VRM and for alerting against the most recent VOI lists received from NAS.

LEAs must not share VOI lists, even in circumstances of NAS unavailability; however, LEAs may share information and intelligence relating to those VOI lists using established intelligence management procedures.

8.9.6. Local system data deletion

Data held on local systems must be deleted within the next 24 hours after the period of 7 days following the time of the read. Where a read is submitted to the local components of NAC more than 7 days after the time of the read by a camera it may be retained for no more than 48 hours in local systems and then deleted within the subsequent 24 hours.

8.9.7. Extended unavailability of NAS

In the unlikely event that connections to the NAS are unavailable for more than 7 days, then deletion of data in accordance with the above provisions may be suspended until such time as connection is restored. This may only be done with specific authority of the controller for the LEA collecting the data and a full written record of the granting of that authority is required.

8.9.8. Mobile ANPR Systems Data Transfer

All ANPR data held on mobile ANPR units that have been unable to transmit their data in real time must be transferred to the NAS within a maximum period of 48 hours from the time of capture except in circumstances where the camera is unable to connect to the local system.

8.9.9. Support and Maintenance

ANPR systems should be commissioned only with an appropriate level of support and maintenance to safeguard against component failure and assist with business change. Local provisions must be in place to ensure that, in the event of any failure of a component of infrastructure that provides communications to the NAS, to prevent loss of data. Reinstatement must be within a period consistent with the ability to retain data locally for that failed component and subject to a maximum period of 72 hours from the time that the component failed.

8.10. System Connectivity

8.10.1. Local ANPR Infrastructure Connectivity to LEA networks

Local ANPR Infrastructure must connect to the LEA network infrastructure to allow user access to the NAS and to support connections to the Police National Computer (PNC) and the NAS.

The security of all infrastructure connections must be managed via an organisation maintained and managed firewall in accordance with that organisation's own policy and the Community Code of Connection and NPCC/Police Scotland Community Security Policy.

8.11. National Databases

NAS must have the capacity to check against the following national databases, as a minimum; PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

8.11.1. Response Times

In order to ensure compliance with DPA principles in the circulation of VOI, Real-time matching performance standards must be achieved in 95% of all reads.

The following table summarises maximum response times within the NAC:

System Type	Read to alarm	Number plate read by a camera to delivery to NAS	NAS process to delivery at a LEA for visibility by staff
Static ANPR system	4 sec	2 sec	2 sec
Moveable ANPR system	4 sec	2 sec	2 sec
Multi-Lane ANPR System	4 sec	2 sec	2 sec
CCTV Integrated ANPR system	4 sec	2 sec	2 sec
Mobile ANPR system	6 sec	4 sec	2 sec

8.11.2. Real-Time Data Delivery

In order to ensure operational capability and to support compliance with DPA, local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8.11.3. Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using criteria defined in TSpec.:

The ability to export ANPR data shall be limited to defined users.

In appropriate circumstances a message may be sent to authorised users by means of SMS text. Where SMS is used the information provided will be limited to the VRM, time and location of the read and the name of the list containing the VOI.

Bulk data, including images, required for investigative purposes that is stored under provisions of the Criminal Procedure and Investigation Act 1996 (CPIA) may be exported to an external LEA defined storage area and managed in accordance with local policy.

The NAS must provide for user defined privileges for use of data export functions and data may only be exported by users with those privileges.

8.11.4. Security

The NAC must provide for adequate security measures, including access control, to protect against unauthorised access to the system and data held within it. LEAs must ensure compliance with NAC requirements and are accountable for the security of all components of the NAC that are within their control. LEAs must ensure that individual user privileges are consistent with the requirements of their role and individual level of vetting.

Audit trails must be maintained to record all significant actions taken, including:

- User login,
- Successful and failed database searches, and;
- the addition to, and deletion of data from lists of VOI.

There must be provision within the NAS for users to record the reasons and any required authorisation for their actions. Access to audit trails must also be auditable and restricted to users who require this access as part of their role, as defined within policy.

The security of all LEA components of the NAC must be managed via an LEA. The LEA shall maintain and manage a firewall in accordance with the LEA's own policy, the Community Code of Connection and Community Security Policy. The requirements of the national network connections and GSC as confirmed by the appropriate governance authority in each case.

8.12. Databases

8.12.1. National Database

LEAs that receive VOI lists and updates from a national VOI list shall ensure that this list is loaded on their mobile system at the first opportunity following receipt of that list or update.

8.12.2. Third Party Databases

Where data is provided by a third party (e.g. the MIDAS File as provided from the Motor Insurance database), then there must be measures/procedures to ensure that the data is handled consistent with these standards. The criteria that must be addressed through these procedures include:

- Provisions must be in place to ensure that only the most up-to-date data set is in use.
- Version control and file naming systems must be in place
- Distribution methods must be in accordance with GSC security requirements.

8.13. Lists of Vehicles of Interest

8.13.1. Vehicle of Interest List Purpose

Lists of Vehicles of Interest (VOI) may be maintained by LEAs to support intelligence development, operations and investigations. The contents of a list of VOI will depend upon the purpose of that list, the format for which is detailed in TSpec.

8.13.2. Vehicle of Interest List Information and Access Controls

VOI Lists used for monitoring purposes and that do not require an operational response may include the details defined within the Tspec. When a VOI List is used to support operational response, sufficient information to ensure an appropriate response must be included.

LEA may maintain a VOI list for operational response purposes; however, these lists should only be used in circumstances that do not meet the need to include the information on the PNC. Access permissions for those lists must be restricted to ensure that data access is proportionate in each case.

Special Categories of Data and Criminal Convictions Data as defined by Schedule 1 of the DPA and Articles 9.1 and 10 of GDPR should only be included within a VOI list when it is essential to the purpose of circulation. The LEA circulating the list must ensure that the content and provisions for the access to any such list are appropriate at all times.

8.13.3. Vehicle of Interest List Resilience

The NAS will make lists of VOI available to LEA in order that they can be loaded onto management servers and mobile systems should the live-link to NAS become unavailable.

LEAs must not load VOI lists received from NAS onto any other systems and must establish procedures to ensure that VOI lists loaded onto the management server or mobile systems are current versions of those lists.

8.13.4. Actions required for a Vehicle of Interest List

Any LEA publishing a list of VOI onto NAS will determine access controls for that list. Lists will only be accessible to LEAs where it is proportionate for that accessibility. Where one LEA subscribes to the VOI Lists of another LEA, there is an obligation to monitor the list, assess a 'hit' against the list and respond subject to local resource availability and operational demands.

Logs of the loading of any VOI list onto a mobile system shall be maintained as required by Section 9.10.

8.13.5. Vehicle of Interest List Accuracy

The LEA supplying a VOI list to the NAS must ensure that information within the list is accurate, of current relevance, and is in a format that conforms to the requirements detailed within TSpec. All lists that are supplied must be reviewed on a regular basis by the LEA supplying the list.

8.13.6. Vehicle of Interest List Deletion

A list that is received from an LEA will be deleted from the NAS no later than 28 days after the last date of revision by the LEA that supplied the list.

8.13.7. Vehicle of Interest List Extraction

LEAs will not extract data from a list of VOI for the purposes of creating a composite list from a number of such lists, to be held outside the NAS.

8.14. Performance Evaluation

Performance testing must be consistent with current guidance provided by the Defence Science and Technology Laboratory (DSTL). (DSTL Guidance)

8.14.1. Installation of ANPR Infrastructure

Unless the exceptions for covert systems apply, on installation of any component of ANPR Infrastructure compliance with performance standards detailed within NASPLE must be confirmed and recorded.

Compliance with performance standards is required for both initial installation or on re-installation or re-deployment of any ANPR camera or other component.

8.14.2. Capture Rate Assessment

Any assessment of ‘capture’ rate must be based on not less than 250 consecutive vehicles (or a minimum period of 2 hours) displaying a VRM visible to the human eye passing within the field of view for a camera and in the case of a multi-lane system this applies to each lane covered by that system.

8.14.3. READ Rate Assessment

The READ rate for each type of system must be determined for not less than 250 consecutive ‘captured’ Vehicles displaying a VRM visible to the human eye.

Performance must be assessed for daylight and night time conditions. It is advisable to assess for a range of conditions including; bright daylight (dawn); bright daylight (dusk); overcast daylight and night time.

8.14.4. Performance Evaluation Schedules

The performance of all ANPR systems must be regularly reviewed to ensure conformance with the data standards defined in this document. NAS functionality should be used to monitor continued compliance with required 'capture' rates.

Compliance with the READ rate for a camera should be reviewed at least annually with a sample of not less than 250 consecutive reads. Provisions for performance evaluation must be defined in LEA policy and procedures.

In addition to the annual assessments, the performance standards for all cameras that do not have the capability to provide supporting imagery must be evaluated at no less than 6 monthly intervals. Assessments for this additional assessment shall include a sample of east 50 vehicles passing consecutively within the field of view.

8.14.5. Performance Evaluation of Covert Cameras

Where covert installation of ANPR infrastructure has been authorised within the provisions of RIPA or RIPSA, and the purpose of the installation may be compromised as a result of testing, the testing need not be completed.

8.14.6. Performance Evaluation Logs

A log for all performance evaluation activities must be retained in a form to enable the record of reviews for each component within ANPR systems to be identified and retrieved when required.

9. Part 3: Data Access and Management Standards

9.1. Data Access and Management Standards Overview

Part 3 prescribes the standards required for access to and management of ANPR data within the NAS.

The obligations that arise under the DPA are different depending on the reason for processing of data. It is the responsibility of the controller for the LEA that is processing the data to ensure compliance with relevant parts of the DPA in each case.

9.2. Data Management

9.2.1. Policy

All LEAs that connect to, or have access to, the NAS must have an up to date written policy in place for the access, management and use of ANPR data, including provisions for audit, which must be consistent with Compliance and Audit Standards.

Access to ANPR data must be proportionate to the circumstances of that access and taking account of the impact on the fundamental rights and freedoms of individuals.

9.2.2. Data Access Management

Authorised members of LEAs may access and use data within the NAS to the extent that is compliant with the DPA in the circumstances of each case, without reference to a controller unless otherwise required within the terms of NASPLE.

9.2.3. Shared Collection Equipment

9.2.3.1. Data provision by non-LEAs

NAS may receive data via an LEA from ANPR systems not directly within the control of the LEA in circumstances where it is using shared collection equipment that is owned and managed by a non-LEA organisation.

In these circumstances, the controller for the LEA that initially receives the data and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently. LEA controllers for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user of the shared collection equipment.

9.2.3.2. Data received directly into NAS

NAS may receive data directly from ANPR systems not within the control of an LEA in circumstances where data is submitted to the NAS using shared collection equipment that is owned and managed by a non-LEA organisation, without the data first being received by a LEA.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment

9.2.3.3. Management of data provided by non-LEAs

In circumstances where a non-LEA has provided data to the NAS, the NPCC policing lead for ANPR and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment.

9.2.3.4. Compliance Agreement

The LEA that receives data from a non-LEA organisation for submission into NAS, or the NPCC policing lead for ANPR in respect of data submitted directly to NAS, must ensure that a formal written-agreement is in place with the owner of the camera and other components of the ANPR infrastructure detailing appropriate arrangements to enable compliance with NASPLE.

9.2.4. Data Extraction from NAS

Where an LEA accesses data within the NAS they are controller for any data extracted from the NAS as a result of that access. Management of all data that is extracted must be in accordance with the provisions within NASPLE and any reports or other documents that include data from NAS must be marked in accordance with the requirements of the Government Security Classifications (GSC). Personal data must only be processed in accordance with the DPA.

9.3. Organisational and User Access to ANPR Data

9.3.1. ANPR Password Policy

Password requirements for access to NAS is based on national Cyber Security Centre guidelines and is applicable to all roles within LEA, third party contractors and suppliers and staff responsible for NAS service management.

Staff will be allocated individual accounts that may only be accessed using a password in a format approved by the national Accreditor to requirements detailed in Appendix A

9.3.2. ANPR Account Management

Staff who are approved to access NAS as both a user and for administrative purposes must be allocated separate accounts such that these functions cannot be achieved using a single log in account. Accounts must be reviewed, suspended or terminated in the following circumstances:

- An account must be suspended if it is not accessed for a period of 90 days. The need for access must be reviewed within the subsequent 7 days. The account may then be reactivated or deleted as appropriate,
- Access permissions must be reviewed within 7 days of a person changing role within an LEA.
- An account must be terminated within a maximum of 48 hours of a person leaving an LEA or partner agency.

9.3.3. Provisions for Data access

Any access to data must be for national security, counter terrorism, investigation and enforcement purposes as defined in Annex B or for the purpose of audit.

Staff within an LEA may be granted access to the extent relevant to their role, in accordance with local LEA policy in an LEA. LEA policy must be consistent with the purposes and standards within this document and the specific requirements at Annex C.

9.3.4. Data Access provision when NAS is unavailable

Data held within the local components of the NAC (Section 8.9) may only be accessed by authorised staff in circumstances where the NAS or communications to the NAS have become unavailable.

9.3.5. Vetting Requirements for access to ANPR data

Staff accessing the NAC are required to have successfully completed vetting to the standards as detailed below unless in exceptional circumstances with express written approval of the NPCC Policing lead for ANPR, as lead controller, approves any vetting process as equivalent to the required standard.

9.3.5.1. Police

Staff within a police service LEA authorised to access ANPR data must have successfully completed Recruitment Vetting (RV) to NPCC vetting standards.

9.3.5.2. Non - Police LEA

Staff within an Approved Organisation that is a non-police LEA authorised to access ANPR data must have current vetting clearance to national non-police personnel vetting (NPPV) Level 2.

9.3.5.3. Partner Agencies

Controllers may allow access to non-police staff in partner agency (e.g. local authority controllers) subject to have them having current vetting clearance to NPPV Level 2, to the extent necessary for their role.

9.3.5.4. Police Service Administration, Monitoring and Audit

Police LEA staff conducting activity in respect of administration, monitoring and audit of the NAS will have a current security clearance to SC level and NPPV to Management Vetting standard.

9.3.5.5. Non-Police LEA Administration, Monitoring and Audit

Non-police LEA staff conducting activity in respect of administration; monitoring and audit of the NAS will have a current security clearance to SC level and NPPV Level 3.

9.3.5.6. National Audit

Staff appointed to any National Audit role must have a minimum current security clearance to Developed Vetting (DV) level and NPPV Level 3.

9.3.5.7. National Administration and Processor Companies

Staff within NAS supplier companies or the Home Office that have access to the NAS for management or administrative purposes will have a current security clearance to SC level and NPPV Level 3.

9.3.6. Authorisation Requirements for access to NAS Data

Where an authorisation for access is required, staff providing that authorisation must ensure that access is proportionate in each case taking account of the DPA and associated principles and that access is in the interest of justice.

9.3.6.1. Authorisation of Staff Access

Each LEA will designate a senior manager who is accountable for the authorisation of staff who may access ANPR data.

9.3.6.2. Role Based Access and Training

Personnel will only be granted access to ANPR data to an extent that is necessary and proportionate to their role. LEAs must ensure that authorised staffs have

completed any required training and are fully aware of the provisions within NASPLE. Authorised staff will have individual access accounts and permissions.

9.3.6.3. Records of Authorised Staff

LEAs will maintain a list of authorised staff and ensure that a persons' authorisation is revised or cancelled as appropriate when they change role or leave the organisation.

9.4. Disclosure and Evidential Use of Data

Data held within or obtained from the NAS may not be used or disclosed for any purposes except those as authorised within NASPLE.

9.4.1. Disclosure schedules

Where ANPR data obtained is retained as material within the meaning of the CPIA (or similar procedures in Scotland), in preparation of disclosure schedules, information relating to ANPR methodology, tactics and camera locations will be recorded on the Schedule of Sensitive Material and may be disclosed to prosecution authorities.

9.4.2. Restrictions on personnel in disclosure of ANPR and in production of evidential materials

Statements of evidence in respect of data within the NAS may only be provided by staff authorised within LEAs to provide ANPR evidence with current access permissions within NAS for that purpose. Subject to the following authorised staff may provide a statement of evidence for any data held within the NAS.

9.4.3. Provisions to safeguard the location of ANPR infrastructure

The order to safeguard the national ANPR infrastructure, apart from data obtained from a Mobile ANPR system, the precise location for an ANPR read obtained from a camera will not be disclosed during an investigation, nor included in evidence unless the controller with responsibility for the camera that recorded the data has been consulted and provided written consent for that disclosure or for evidence to be provided. The following principles apply:

9.4.3.1. Evidential Use of Data

Evidence of an ANPR read will only be included where it is of specific relevance to an investigation and is of material value to any judicial proceedings.

9.4.3.2. Disclosing of Camera Locations in Evidence

Apart from data obtained from a Mobile ANPR system the production of a map or otherwise disclosing the precise location of the camera that recorded an ANPR read is not permitted during any stage of an investigative or prosecution process, unless

specifically authorised by the data controller for the LEA with responsibility for the camera that recorded that data.

9.4.3.3. Information to be included in evidential disclosure

The location of a read will be described in the following decreasing order of preference;

1. The general area of the location (e.g. Town, District, Metropolitan Borough)
2. The postcode (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)
3. The name of the road (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)
4. The precise location (following consultation with the controller with responsibility for the camera that recorded the data)

9.4.3.4. Disclosure of ANPR data for non-evidential purposes

Unless permitted within section 9.6 of this document, core ANPR read data and any supporting imagery as defined by section 7.4.5., is not to be transferred to other systems, nor disclosed to any third party, including staff from an organisation that is not listed at Annex A, Data may only be disclosed to the data subject in accordance with procedures for dealing with FOI and DPA enquiries in accordance with section 9.12. Data may be shared with an organisation that is not listed at Annex A with the express written authority of the controller with responsibility for the camera that recorded that data.

9.4.3.5. Disclosure to non-Approved Organisations

Where an LEA has an active role in collaboration with another LEA which is not listed at Annex A in the conduct of an investigation, and circumstances consistent with the provisions of Schedule 2 DPA apply, the results of a search of ANPR data may be disclosed to that other LEA with a requirement that it is not further disclosed without the express written authority of the controller for the 'Approved Organisation' collaborating in the investigation.

9.4.3.6. Controller Representations re Disclosure of Camera Locations

In addition to the above, the controller that owns or controls the camera that captures 'read' data will be provided with a specific opportunity to make representation to any court that is to consider an order for information to be disclosed regarding the location of a camera.

9.4.3.7. Recording of Disclosure

In all circumstances where data is disclosed a record must be maintained to include the identity of those disclosing and receiving the data and the reason for and any authorisation of that disclosure.

9.5. Retention and Deletion

9.5.1. Record Retention and Deletion

ANPR READ records must be deleted 12 months[4] after their initial capture, unless retained under provisions of CPIA or similar provisions in Scotland. Retained data may only be accessed in connection with the investigation subject to that retention after a period of 12 months following initial capture.

Records may also be retained for longer than 12 months following a review that identifies a continuing policing purpose for those items of data under provisions of MOPI. These records must be retained and managed in accordance with those provisions. LEAs must establish procedures for the management and review of any data held under these provisions including arrangements for deletion as required.

9.6. Storage of ANPR Data otherwise than in NAS

Data must not be stored outside the NAS except where held in buffer storage in accordance with section 8.9.5 unless for the purpose of retention in accordance with section 9.5.1 or in accordance with section 9.8 below where those requirements cannot be met within the NAS, or it has been extracted as a result of a court order or other lawful authority for the provision of the data.

9.7. Record Amendment

Records that are identified as incorrect for any reason must either be corrected or deleted at the time that they are found to be incorrect.

9.8. Record Deletion from Third Party Systems

ANPR data must be deleted from any computer-based system within 7 days of entry of that data, where an LEA has established any link between the NAS and any other computer-based system for the purposes of:

- Monitoring and the initiation of an operational response to any hit against a list of vehicles of interest or

[4] Read metadata is deleted on day 366 after initial capture. Associated images are deleted the following day. Data may only be accessed up to 12 months after initial capture (Annex C) unless in circumstances of 9.5.1 above.

- More advanced research and analysis purposes in relation to an investigation.
- Entries are included in command and control records

An exception exists for deletion after 7 days when a review has been conducted of the data that it is proposed to be retained which has identified the items of data where a continued policing purpose remains that can only be satisfied by the continued processing of the data within the system external to the NAS.

In this case provisions of MOPI (or similar provisions in Scotland) apply and the relevant items of data may be retained and managed in accordance with those provisions; or

An exception also exists for deletion after 7 days when a review has been conducted into the data that it is proposed to be retained which has confirmed that the items of data are relevant to an investigation. In this case the relevant items of data may be retained, managed and deleted in accordance with the requirements of CPIA.

9.9. Transfer to local systems for basic user access

Data may not be transferred to any local systems external to those required for connection to NAS facilitate basic user access to ANPR data.

9.10. Records of Data Processing, Access and Disclosure

9.10.1. NAS Logging

A log of all automated processing operations will be maintained within NAS to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access.

9.10.2. Mobile Systems Logging

A log recording the details of all lists of VOI that have been loaded onto mobile systems as authorised by section 8.9.8 will be maintained by the LEA that loaded the log onto the mobile systems.

9.10.3. Logging of Access on systems external to NAS

In addition, LEAs are required to maintain a record of any access by their staff to ANPR data, in any external system, to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access in a readily retrievable form.

9.10.4. Logging of Escalation of Investigation Category

LEAs are required to maintain a record of any escalation of an investigation to the category 'Major Investigation' or 'Serious Investigation', including details of the reason for escalation, in a readily retrievable form.

9.10.5. Logging of data Disclosures

Unless disclosure is in accordance with the provisions of the CPIA or similar provisions in Scotland, LEAs will maintain records of all disclosure of ANPR data including the justification, data and time of the disclosure, the identity of the person disclosing the data and the identity of the recipient of the data.

9.10.6. Use of Logs in Disciplinary Proceedings

Logs within NAS and those recorded by an LEA may be used for the purposes of self-monitoring by the controller or the processor, the conduct of internal disciplinary proceedings, in ensuring the integrity and security of personal data and for the purposes of criminal proceedings.

9.10.7. Disclosure of Logs to ICO, SCC and Home Office

Records within NAS and any local records must be made available to the Information Commissioner, the Surveillance Camera Commissioner and the Home Office on request for audit and monitoring purposes.

9.11. Management and Audit of NAS

Audit must be conducted in accordance with National Standards for Compliance and Audit of Law Enforcement ANPR by staff with appropriate security clearance.

LEAs will support all controllers for NAS in the audit and management of NAS.

LEAs will support the national auditor in the monitoring and audit of access to the NAS and will provide relevant information on request.

LEAs will audit the access to NAS by their staff in accordance with Audit Standards and maintain a record of all audits that are undertaken. Details of such audits will be made available to the Information Commissioner, the Surveillance Camera Commissioner and the national auditors on request.

9.12. Freedom of Information Act and Data Protection Act Enquiries

All requests for Information regarding the NAS made to a public authority under the provisions of the Freedom of Information Act 2000 (FOI) will be referred to the relevant controller for consideration and will be managed according to the JCA.

All requests in relation to data held on NAS, made under provision of the DPA, will be referred to the controller for consideration and will be managed according to the

JCA. This includes any subject access requests and requests for erasure or restriction on processing.

Annex A: Approved Organisations

List of Approved Organisations
Avon and Somerset Constabulary
Bedfordshire Police
Border Force
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Department for Work and Pensions (DWP)
Derbyshire Constabulary
Devon and Cornwall Constabulary
Dorset Police
Driver and Vehicle Licensing Agency (DVLA)
Driver and Vehicle Standards Agency (DVSA)
Durham Constabulary
Dyfed-Powys Police
Environment Agency
Essex Police
Food Standards Agency
Gangmasters and Labour Abuse Authority
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
H M Revenue & Customs (HMRC)
Humberside Police
Immigration Enforcement
Intelligence Services
Kent Police

Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Medicines and Healthcare Products Regulatory Agency (MHRA)
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
National Crime Agency (NCA)
NAFN Data and Intelligence Services facilitating Local Authority Trading Standards investigations
National Vehicle Crime Intelligence Service (NaVCIS)
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Scotland
Police Service of Northern Ireland (PSNI)
Royal Air Force Police
Royal Military Police
Royal Navy Police
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Thurrock National Investigation Service
Warwickshire Police
West Mercia Constabulary
West Midlands Police
West Yorkshire Police
Wiltshire Police

Annex B: Investigation Categories

Investigations within LEAs fall within three main categories, so that there is a consistency of understanding within LEAs as to which investigations should be included within each category. The main categories are:

- Major Investigations
- Serious Investigations
- Priority and Volume Investigations

A consideration of the category of the investigation informs effective management and decision making, including the scope for an investigation and determination of the resources that are to be deployed. These categories provide the framework to support a national policy for retention of, and access to ANPR data. The categorisation of an investigation should be determined taking account of the circumstances in each case, using the below framework as a guide.

Major Investigations

A key characteristic is that Major Investigations should be normally be led by a Nationally Registered Senior Investigating Officer (SIO) within a police force or similarly senior investigator in non-police LEAs.

Designated Major Investigations

Major Investigation Types
Murder
Attempted Murder
Manslaughter
Infanticide
Child Destruction
Kidnapping

Terrorist related crimes

Serious Investigations

Designated Serious Investigations

Serious Investigation Types
Arson
Abduction
Aggravated Burglary dwelling and non-dwelling
Arson High Value or life endangered
Blackmail
Drug Trafficking
Death by Dangerous Driving
Female Genital Mutilation
Fraud and Associated Offences (80hrs + investigation time)
Gross Indecency Child
Perverting Justice
Public order (racially motivated)
Rape
Robbery (Firearms or ABH or more serious injury caused)
Sexual Assault (children under 13)
Threats to Kill
Vulnerable Missing Person

Wounding (S18/20)
Response to incidents of significant public interest / public safety/ public security

Serious Investigation Escalation

Serious Investigations may, with the authority of a senior manager[5] be escalated to the category of Major Investigations.

Investigations that have been escalated to serious from the category of Priority and Volume Investigations may not be further escalated to the category of major Investigation.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded. Any authority to escalate will take account of the following factors:

Serious Investigation Escalation Factors

Consideration	Examples
Community factors	• Likely to escalate into large scale disorder or critical incident • Has escalated from a previous offence • Sensitivity regarding individuals involved
Offence characteristics	• Aggravating factors of the offence • Vulnerability of victims/witnesses, • Has crossed force or national boundaries • Forms a previously undetected series

[5] an officer of at least superintendent rank in the police or the equivalent level of seniority in a non-police organisation

Offender Characteristics	• Organised crime • Terrorism links • Resistance to police operational strategies • Multiple offenders

Priority and Volume Investigations

Investigations not included within the above categories will be considered as within the remit of Priority and Volume Investigations. This will include investigations into street robbery, burglary and vehicle-related criminality and non-crime issues such as anti-social behaviour, vehicle excise enforcement, road traffic offences, safeguarding and missing persons.

Priority and Volume Investigations may with the authority of manager[6], be escalated to the category of Serious Investigations.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded and will take account of the following factors:

Priority and Volume Investigations Escalation Factors

Consideration	Examples
Community	• **High risk of critical incident** • **Sensitivity regarding individuals involved**

[6] an officer of at least Inspector rank in the police or the equivalent level of seniority in a non-police organisation

Offence Characteristics	• Aggravating factors of the offence such as: • Hate crime • Weapons used • Injuries sustained • Vulnerability of victims/witnesses, • Priority issue identified within NIM business process. • Series of offences e.g. forensic links to the offender(s) • Complexity of the Investigation
Offender Characteristics	• Criminal history • Resistance to investigative strategies • Prolific offender • Multiple offenders

Annex C: Data Access Requirements

Age of data to be accessed (as required)	Purpose of access to data
	To monitor alarms or receive reports from matches against a list of Vehicles of Interest (VOI) from a NRD for operational response or intelligence purposes.
Real or near real time during the course of monitoring	By any member of staff authorised to access ANPR systems with no additional authority required.
	To research data for 'Priority and Volume Investigation' purposes.
Up to 90 days	By any member of staff in accordance with their authorisation to access ANPR systems.
Over 90 days	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of an Inspector or equivalent staff grade; a) where there has been a significant delay in reporting the offence to be investigated, or; b) new information or evidence has become available, or; c) the investigation is being conducted diligently and expeditiously and is not yet completed.
	To research data for 'Serious Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.

	To research data for 'National Security', 'Counter Terrorism' or other 'Major Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.
	To prepare evidential material for information revealed during a previous search of ANPR data.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To comply with a written request from the Crown Prosecution Service, the procurator fiscal or on the direction of a court.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To research data as part of an investigation into alleged breach of the policing Code of Ethics
	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of a superintendent or equivalent staff grade.

Appendix A: Password Requirements

Password Requirements

Introduction

Purpose

1. The security of NAS requires that users generate an appropriately complex password to protect the National ANPR Capability (NAC) and its data from unauthorised access. The NAS utilises a username and password-based identity and access control for all front-end users.
2. The NAS Password Policy is a procedural part of the information security measures intended to:
    - Protect the Confidentiality, Integrity and Availability of the NAC.
    - Preserve the privacy of all the data and information stored within the NAC environment, ensuring only authorised users are permitted access on a need to know basis.

Procedures

The Purpose of Passwords

3. Passwords are an essential security control to authenticate users and confirm identity and access rights. Passwords protect access to the ANPR data and information in conjunction with the physical and procedural measures of a secure site.
4. Visual recognition of people within a work area, and Photographic ID Cards for sites and buildings, are also an important security layer to protect the NAC.

Limitations

5. The security provided by a password system requires the passwords are known only to the user of the account to which it relates. Thus, a password is vulnerable to compromise whenever it is stored or written down. A user must not disclose their password to anyone including other users and administrators.

Password Requirements

Password creation requirements:

6. Passwords **must** be a minimum length of 8 characters with at least 2 non-alphanumeric characters (e.g. % & ?);
7. Passwords **must not** be stored in any insecure form, users must **disable** password saving in web browsers;
8. Passwords **must not** be based on the following:
   - Months of the year, days of the week or any aspect of dates with which they are personally associated (e.g. birthdays, anniversaries);
   - Family names, initials or car registration numbers;
   - Organisation names, identifiers or references;
9. Good quality passwords should:
   - Not be the same as any of the previous 10 passwords (this will be enforced via the operating system or security solution within NAC);
   - Be unique and only used within the NAC;
10. Password must be changed on suspicion of compromise;
11. Password creation requirements are common for all types of NAC access. If a user has more than one account. For example, a user administrator and system administrator account, different passwords are required for each account;

Expiry terms and Account Lockout

	No of Attempts	*Password expiry*
User/ Role	5	1yr

12. If a user has attempted to log in **5 times** unsuccessfully their account will be:

    a. **Locked out** and **ONLY** unlocked via two alternative processes for use depending upon the business processes of the LEA:
       i. Notify the local User Administrator or,
       ii. Notify the local LEA IT Service Desk.

Forgotten Password Process

13. If a user has forgotten password, A **"I forgot my password"** link is provided on the NAS logon homepage. The system will email a new temporary password to the email address associated with the NAS user account. This temporary password **must** be immediately changed upon first successful login. This will not circumvent the lockout procedure described above.



© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications and www.npcc.police.uk/anpr

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk .

GOV.UK

1. Home (https://www.gov.uk/)
2. Crime, justice and law (https://www.gov.uk/crime-justice-and-law)
3. National ANPR standards (https://www.gov.uk/government/publications/national-anpr-standards)

- Home Office (https://www.gov.uk/government/organisations/home-office)

Guidance

National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version)

Updated 19 November 2020

Contents

1. Purpose of Compliance and Audit
2. Applicability
3. Audit Governance and Roles
4. Data Standards Audit
5. Infrastructure Standards Audit
6. LEA Local System Audit
7. Vehicle of Interest (VOI) lists Audit
8. Data Access and Management Standards Audit
9. Glossary of Terms, Abbreviations and Definitions
10. Document revisions

Print this page

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 (https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/publications/national-anpr-standards/national-standards-for-compliance-and-audit-of-law-enforcement-anpr-july-2019

1. Purpose of Compliance and Audit

Consistent management of NAS is essential to ensure that data is accurate and to maximise the benefits for law enforcement purposes. Public confidence in the system is essential and robust standards with clear records of compliance with those standards is importance to ensure support for ANPR systems is maintained.

Audit is one part of a larger suite of security controls and measures which includes, governance, physical, personnel, technical and procedural controls. The NAS is designed to provide a security regime that supports and compliments the business and technical needs. It is important that business audit standards, policy and governance are also in place which requires a robust compliance audit regime to be in place.

2. Applicability

These Audit Standards apply to national law enforcement ANPR capability (NAC) operated by the police and other law enforcement agencies (hereinafter called LEA), throughout the UK, that connect to or receive data from the National ANPR Service (NAS).

Audit is conducted with reference to National Standards for Policing and Law Enforcement (NASPLE)

LEAs must ensure compliance by their agency with the requirements of all parts of NASPLE.

3. Audit Governance and Roles

The National Strategic lead as lead controller must ensure that audit standards are in place to provide for effective governance of NAS taking account of threats and risks.

Staff conducting audits must have current security clearance to levels as detailed in NASPLE Part 3.

Staff with user access permissions to NAS may not conduct audits.

LEA must ensure that audit of any access to NAS using administrative permissions is conducted by staff who do not themselves have administrative responsibility for NAS.

3.1 Governance model

The below governance model is in place for NAS:

The National ANPR Strategy Board supports the NPCC Strategic Lead.

The National ANPR Advisory Board advises the NPCC Strategic Lead.

The NAS Service Management reports to the NPCC Strategic Lead.

The National Accreditor reports to the NPCC Strategic Lead.

The National Auditor reports to the NPCC Strategic Lead.

The National Accreditor advises the Security and Data Management within Strategic Board.

906

The National Auditor advises the Security and Data Management within Strategic Board.

The Security and Data Management within Strategic Board advises the NAS Service Management.

The National Auditor audits the activity of National System Providers and the National Administrator.

The National Auditor monitors the activity of local auditors.

The Service Desk oversees the National System Providers.

The National Administrator supports and advises the Local Administrators.

Local Auditors audit users.

4. Data Standards Audit

Accurate data is essential to ensure legislative compliance and to enable the benefits that can be obtained from ANPR to be optimised. The following elements of NASPLE Part 1 are included for audit.

4.1 Data Security

Every 6 months LEA to review a sample of reports that have been obtained by that LEA from NAS for compliance with the requirements of the Government Security.

Classification Policy (GSCP) requirements for OFFICIAL – SENSITIVE data. (NAS configuration should ensure that all reports are appropriately marked).

4.2 Time

LEAs must record evidence of the accuracy of time recording for all camera that submit data to their management server. Records confirmation of time accuracy must be reviewed at Least once every 7 days. A record of review and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.3 Location

The accuracy of the recording of location for a read record from all camera with the exception of mobile camera must be confirmed on installation and thereafter reviewed at Least once every 6 months by the LEA manging that camera. A record of all reviews and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.4 Reporting of Data Standards

Every 12 months LEA must provide the national auditor with a report to include details of the number of cameras operated by the LEA, the number tested during the preceding 12 months, information of the accuracy for recording time and location for each camera tested and details of any maintenance conducted following testing.

5. Infrastructure Standards Audit

5.1 ANPR Infrastructure Development

Compliance with NASPLE Part 2 is important to ensure that ANPR systems are developed and maintained in conformance with relevant legislation and that the benefits that can be obtained from the NAS are optimised. The following elements of NASPLE Part 2 are included for audit.

5.2 Static ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14 LEAs to retain records of all reviews for a period of 2 years.

5.3 Moveable ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.4 Multi Lane ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.5 CCTV Integrated ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.6 Mobile ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.7 Covert Systems

Audit of deployments of ANPR systems authorised within provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) to be completed in accordance with arrangements for compliance and review of RIPA and RIPSA deployments as appropriate.

6. LEA Local System Audit

6.1 Local Systems

Audit of local data storage to be completed by the LEA every 6 months to confirm that the period of retention is consistent with NASPLE Part 2 and that data is not transferred or used in other systems except as authorised by NASPLE.

6.2 Mobile Systems Data Transfer

Review of records for transfer of data from Mobile ANPR Systems to be completed by the LEA every 7 days to confirm compliance with NASPLE Part 2. LEAs to retain records of all reviews for a period of 2 years.

6.3 Support and Maintenance

Records for failure of any component of infrastructure to be reviewed by the LEA every 7 days to support compliance with requirements for reinstatement of capability as detailed in NASPLE section 8.14.

7. Vehicle of Interest (VOI) lists Audit

Compliance with the requirement for deletion of lists from NAS 28 days after the latest date of revision to be reviewed by the LEA every 14 days.

Lists held on Mobile ANPR Systems to be reviewed by the LEA at Least once every 7 days to ensure that they remain the current version of any VOI list.

LEA to maintain a record for the review of all VOI lists and retain those records for a period of 2 years.

8. Data Access and Management Standards Audit

8.1 Policy

Annually, the local auditor to confirm that a current written policy is in place in accordance with NASPLE Part 3.

8.2 Audit of provisions for Data Access

The identity of the senior manager as required by NASPLE Section 9.3.6.1 to be confirmed by the local auditor annually

Evidence of the management of staff authorisations and permissions to be audited by the LEA for compliance with authorisation and removal procedures to include:

- annually 5% of all new staff authorisations that have been approved during the previous 12 months
- annually review a sample of staff authorisations where the privileges have changed during the previous 12 months
- all staff who have not accessed NAS for a period of 90 days within the 14 days immediately following the expiry of that period
- all accounts for staff that have left the LEA within 48 hours of them leaving an LEA to ensure that access permissions have been ceased

- annually all staff with administrative access to ensure that this remains appropriate and is not combined with user access permissions[909]
- monthly to review records for all failed ‘log on’ attempts. A record of all reviews conducted to be retained for a period of 2 years

LEA audit to be conducted every 6 months to confirm the deletion of data in accordance with NASPLE with an annual review of 5% of all cases where data is retained beyond standard deletion times to ensure continued retention remains appropriate, both for NAS and other systems.

LEA to audit of instances of data access to ensure access is appropriate within terms of NASPLE with reference to the justification and authority where required as follows:

- LEAs must establish provisions for audit of ANPR data where the period for the search includes data that entered the NAS 90 days or less prior to the search, that is proportionate in each case taking account of their assessment of the potential risk of non-compliance with NASPLE and for the misuse of data. The audit to be completed quarterly[footnote 1]
- to audit 5% of searches across a sample covering 30 consecutive days since the previous audit where those searches cover data that was captured more than 90 days prior to the date of search. The audit to be completed quarterly
- all instances of access to data preserved under provisions of the Criminal Procedure and Investigations Act 1996 (CPIA)

As a minimum, the following elements of data access must be reviewed as part of the audit:

- that any search was properly authorised where required with evidence of authorisation recorded
- that the timescales for the search were appropriate in that they were no greater than was necessary and proportionate in the circumstances of the investigation
- that the reason, purpose and justification for the search was fully recorded within NAS

In respect of access to data preserved under provisions of the CPIA that any access was solely for the investigation for which it was preserved.

LEAs to audit 10% of records of the disclosure of data otherwise than in accordance with CPIA or similar procedures in Scotland in respect of the justification, the date and time of the disclosure and the identification of both the person disclosing and the recipient of the data. (NASPLE section 9.4.3.7)

LEAs are responsible for dealing with any non-compliance with standards that are identified during audit and must report all non-compliance and a copy of the audit report to the national auditor within 28 days of the non-compliance being identified.

All LEAs must maintain a record of audits that are conducted to include:

- a statement of the findings for all audit activity
- a report of the extent of non-compliance
- a report of action taken in relation to non-compliance

Records of audit will be retained for a period of 2 years and made available to the national auditor on request.

8.3 Audit of Changes to Read Records

LEAs to review a sample of changes to ‘read’ records every 6 months to confirm the validity of the change. Records of review to be retained for a period of 2 years.

8.4 Audit of Access by System Providers, National Administrators and Local Auditors

The National Auditor will audit access to NAS by system providers, national administrators and local auditors, reporting details of any audit that is conducted for the information of controllers to the extent determined by those post holders.

The National Auditor will conduct a NAS system audit every 6 months to confirm data is deleted in line with the requirements of NASPLE Part 2.

Audit of access to NAS by a user with ‘Super Administrator’ permissions will be conducted for each occasion that the system is accessed when those permissions are enabled for that user by the National Auditor.

9. Glossary of Terms, Abbreviations and Definitions

ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture and ANPR read. CPIA Criminal Procedure and Investigations Act 1996
DPA	Data Protection Act 2018
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS))
GPS	Global Positioning System
JPEG	Joint Photographic Expert Group image format
NAS	National ANPR Service
NAC	National Law Enforcement ANPR Capability
NPCC	National Police Chiefs’ Council

NASPLE	National ANPR Standards for Policing and Law Enforcement
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities
Read	The interpretation of a VRM by an ANPR system
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
VRM	Vehicle Registration Mark

10. Document revisions

Version 2.0, September 2020: Update of links within text, Minor revision of section 7

---

1. In most cases a sample of 2% of all instances where the period included in the search extends for 90 days or less prior to the date of the search being conducted for a sample of 30 consecutive days in a period since the previous audit (quarterly) is likely to be appropriate. Depending upon the level of risk a lessor or greater sample may be appropriate. The rationale for determining the data sample should be documented in all cases

Print this page

Home Office

National ANPR Service

National ANPR Service
Technical Specifications

Version 3.0
June 2020

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulations
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Agreement under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format

LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC
NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information

PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

1 Introduction

This document prescribes the technical specifications for data within the National ANPR Service (NAS). National ANPR Standards for Policing and Law Enforcement (NASPLE) set out the standards that are required for the National ANPR Capability (NAC) to ensure compliance with relevant legislation in the operation and use of law enforcement ANPR. The information within this document is intended to support compliance and consistency in the operation and management of NAS by the police and other law enforcement organisations (hereafter referred to as LEA).

2 ANPR Read Records

2.1 System Testing

The only number that may be entered into any component of the NAS for the purpose of testing connectivity is QQ111QQQ.

2.2 Core Data Components

2.2.1 Vehicle Registration Mark (VRM) (Mandatory)

Where a camera has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, 'QQQQQQQ'1 must be recorded within the VRM field.

The required format must conform to the Standard Coding Format UTF-8character set. The VRM must contain no spaces.

2.2.2 Time (Mandatory)

Recorded and synchronised using standard time source techniques to Greenwich Mean Time (GMT) plus 0 (+0) at least once every 10 minutes, with accuracy to stratum level 3.

The required format is 'dd/mm/yyyy hh:mm:ss', in 24 hour format.

2.2.3 Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. This location should have been ascertained through a Global Positioning System (GPS) device. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

[1] Some ANPR cameras can detect the presence of a vehicle where no VRM is visible and the use of 'QQQQQQQ' ensures that these vehicles are traceable in the database with a format that will not be attributed to a genuine VRM.

The required format for recording a location is latitude and longitude in decimal degrees.

When a mobile ANPR system is unable to deliver an accurate GPS coordinate for a read, the GPS field must be populated with N0000000 E00000000.

2.2.4 Supporting imagery

Plate patch – showing the number plate only, (Mandatory for systems under ownership or control of an LEA).

A plate patch must be in JPEG format, 120x60 pixels and be no more than 3kB in size.

Overview – showing the vehicle in the context of the read zone (Optional).

An overview image must be in JPEG format, no more than 25kB in size.

Where images obtained by a camera exceed 3Kb for a plate patch or 25KB for an overview, these must be adjusted prior to forwarding to the NAS.

'Geo Tagging', if an accurate GPS Geo Location is available, then this detail may be added to images using Exif (Exchangeable image file format) (Optional

Other metadata

Column	Format	Mandatory	Details
Feed ID	Numeric	Yes	2 character code as used by the Police National Computer (PNC) Also known as 'Force ID'
Source ID	Numeric	Yes	Short integer (range 1 to 9999)
NRD ID	Numeric	Yes	Short integer (range 0 to 9999) (NRD ID zero (0) must be used to denote VRMs entered manually by an administrator of the ANPR system.)
Lane ID	Alphanumeric	No	Optional text description
'Alias' ID	Alphanumeric	No	Optional textual description that does not disclose the exact location of a NRD
Username	String	Yes	Username of operator using the ANPR system. When deployed in other circumstances, use 'Unattended'.
Preset ID	Integer	No	Short integer Default value is 0 Used to indicate direction of travel on multi-lane CCTV cameras.

3 Data storage and management

3.1 Data loss and resilience

The NAS must not allow any data loss and be configured to provide to provide resilient capability.

3.2 Local system retention and deletion

Local components of NAC must be configured to enable retention of any data received from a camera at more than 7 days for a maximum of 48 hours and for deletion of that data within the following 24 hours.

3.3 Mobile Data Transfer

Local capability must be in place to support transfer of data from mobile ANPR units to the NAS within 48 hours of capture by the camera within the mobile system.

4 National Databases

The NAS must have the technical capability to run the following national databases, as a minimum - PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

PNC Extract File

The PNC Extract File is available to forces at least three times every 24 hours and should be loaded onto the mobile systems opportunity following receipt. All ANPR reads must match against the PNC Extract File should the live link to the PNC be unavailable.

5 Vehicle of Interest (VOI) Lists

VOI lists in NAS will be referenced to the LEA that creates and manages the list. In order to support the display of symbols within vehicle mounted systems the file name will be in accordance with the reference list at Annex A.

The following character mapping is to be used. All lists of VOI must conform to the following template, **(Mandatory elements shown in bold text)**:

NB: Entries in 'Standard Words' section must match **exactly** those in the template for uploading into NAS

Column	Description	Standard Words	Comment
1	**VRM**		No spaces, Alphanumeric characters only
2	MAKE		
3	MODEL		
4	COLOUR		
5	**ACTION**	Stop Assess No Alert	Action can include a requirement to STOP the vehicle and take action as described Or To assess in the context at the time the vehicle comes to notice to determine action. Or No Alert only to be used when a VOI list is submitted for monitoring purposes with no intention that any action is taken when the vehicle comes to notice
6	**WARNING MARKERS**	No Warning Known Warnings Present	Generally, PNC ACTion should be used if warning markers are present. For VOI lists, 'No Warning Known' is most applicable. If it is essential to use a VOI list and warning markers are present then 'Warnings Present' should be used with the agreed PNC abbreviation (max of 3) entered as the first words separated only by a space in the Information /Action field. (field 9)

Column	Description	Standard Words	Comment
7	**REASON**	Intel Serious Crime Cloned Low Crime Drugs Intel Sexual Intel Low Crime Offender management Impaired Driving Documents Disqualified Other No Insurance DO NOT USE No MOT – Do NOT USE No Tax – Do NOT USE No Keeper – Do NOT USE LEA P1 LEA P2 LEA P3 LEA P4 LEA P5 LEA P6	Only one reason code per entry No Insurance, No MOT, No Tax and No Keeper MUST NOT be used as a REASON to create a VOI list entry. If intelligence relates to one of these categories, then DOCUMENTS must be used. They are included in the template solely for the use of nationally populated lists to support NAS functionality.
8	INTEL 3X5X2		Enter grading without X or spaces
9	**INFORMATION/ ACTION**	Free Text – Maximum of 198 characters including spaces and punctuation. Carriage return must not be used	Brief free text sufficient to add extra value and detail for the person dealing with activation.
10	**LEA AND AREA**		Include Force Name/ Area (BCU/Division letter/ other LEA ref
11	**START DATE**	Provide date in format [dd/mm/yyyy]	
12	**WEED DATE**	Provide date in format [dd/mm/yyyy];	Entries will be weeded on date specified
13	PNC ID		
14	**GSC marking**	OFFICIAL (or) OFFICIAL-SENSITIVE	Only one marker to be used
15	CAD		
16	**CONTACT**	Provide details of 24hour point of contact for enquiries if vehicle stopped	

6 Real Time Matching

The NAS must provide real-time matching to PNC and other lists of VOI for all ANPR reads.

The system response time from a Vehicle Registration Mark (VRM) being captured by a camera to the hit notification response being delivered to a specific operator must not exceed 4 seconds for static, moveable, dual lane and CCTV Integrated systems, and 6 seconds for mobile ANPR systems.

To allow for this end-to-end performance requirement, the camera must deliver ANPR reads to the NAS within 2 seconds of capture for static, moveable, dual lane and CCTV ANPR Integrated systems and within 4 seconds of capture for mobile ANPR systems.

The NAS must process that read against the PNC and other VOI databases and deliver any resultant match notification to the operator within 2 seconds of receipt of the read by the NAS for all systems.

7 Real Time Delivery of Data

Local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8 Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using any of the following criteria:

- Vehicle Registration Mark (VRM);
- Date and time parameters;
- by camera identification;
- by location co-ordinates;
- by ‘geo plotting’
- direction of travel (desirable)

9 Interoperability

Systems must enable interoperability between LEAs and the NAS to allow:

- Real-time matching of reads against lists of VOI and the real-time delivery of hits
- Remote research in accordance with prevailing researching guidelines
- NAS read searching for national data searches and data mining in accordance with the NAS Business Rules, as defined within current NASPLE
- Distribution of lists of vehicles of interest to the NAS
- Transfer of data and all associated images between LEA ANPR Infrastructure and the NAS.

Annex A

Vehicle of Interest List (VOI) Naming Convention

In order to display the name of the organisation creating the VOI list within symbols in vehicle mounted systems, character mapping is required. A VOI list file name will begin with the organisations PNC ID followed by an underscore (for example 07_Cheshire VOI List); the agreed force abbreviation will be displayed in the bottom 'white' section of the VOI symbol (in this example CHESH would be displayed). The following character mapping is to be used:

Character at start of VOI File name followed by underscore	***Display in bottom white section of VOI symbol***
52	**A&S**
40	**BEDS**
93	**BTP**
35	**CAMBS**
07	**CHESH**
48	**COLP**
59	**CNC**
17	**CLEV**
03	**CMBRIA**
30	**DERBYS**
50	**D&C**
55	**DORSET**
94	**DVLA**
201	**DVSA**
11	**DURHAM**
63	**DPP**
42	**ESSEX**
53	**GLOS**
06	**GMP**
61	**GWENT**
44	**HANTS**
41	**HERTS**
88	**LEA**
16	**HUMB**
46	**KENT**
04	**LANCS**
33	**LEICS**
32	**LINCS**
05	**MERPOL**
02	**METPOL**
24	**MOD**
36	**NFOLK**
60	**NWP**
12	**NYP**
34	**NHANTS**
10	**NORPOL**
31	**NOTTS**
90	**PSOS**

98	**PSNI**
62	**SWP**
14	**SYP**
21	**STAFFS**
37	**SFFOLK**
45	**SURREY**
47	**SUSSEX**
43	**TVP**
23	**WARWCK**
22	**WMERCA**
20	**WMIDS**
13	**WYP**
54	**WILTS**
LEA	**LEA**
TUTELAGE	**TULAGE**
MIDASGOLD	**MIBGLD**
TRIVIUM	**TRVIUM**

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk

Department of State Police
Special Order

Effective Date	Number
October 1, 2019	**19-SO-12**

Subject

Distribution of General Orders

I. DISTRIBUTION OF GENERAL ORDER

Policy and Procedure
TRF-11 Automatic License Plate Recognition

The requirements for the distribution of the above listed General Order are:

√ Each employee shall follow the instructions within this Special Order.
√ Supervisors shall obtain a signature receipt from each employee acknowledging this General Order has been promulgated and posted on DocuShare.
√ Troop/Station/Section/Unit Commanders shall forward the *completed* signature receipt forms through channels to their respective Division Commanders on or before: November 1, 2019.
√ Division Commanders shall:
- Ensure that employees under their command have been notified of this General Order; and
- Maintain a file of all completed signature receipt forms for their Division.

II. DISTRIBUTION OF GENERAL ORDER INSTRUCTIONS

A. Instructions

Each employee shall acknowledge that the following General Order has been rescinded:

Policy and Procedure		Effective Date
TRF-11	Automatic License Plate Recognition	06/14/2018

III. DISTRIBUTION OF GENERAL ORDER INSTRUCTIONS

A. Instructions

It is the responsibility of each sworn and civilian employee to read promulgated directives. Sworn and civilian employees shall read and become familiar with the contents of all posted written directives.

Each employee shall acknowledge the following General Order has been promulgated and posted to DocuShare. Each employee is responsible for reading and becoming familiar with the following General Order:

Policy and Procedure		Effective Date
TRF-11	Automatic License Plate Recognition	10/01/2019

OFFICIAL:

KERRY A. GILPIN
Colonel/Superintendent

EXAMINING THE PUBLIC SAFETY BENEFITS OF FIXED POSITION LICENSE PLATE READERS (LPRS)

NATIONAL POLICE FOUNDATION



What We Know

Existing research suggests that LPRs can benefit law enforcement, but that the technology's impact depends on its implementation. To date, research has found that LPRs can be an effective tool for improving stolen vehicle recovery and arrests for auto thefts (Koper et al., 2013, 2019, 2021; Ohio State Highway Patrol, 2005; Ozer, 2010; Taylor et al., 2012) and may improve clearance rates for auto theft and robbery cases when used properly (Koper and Lum, 2019).

However, several studies exploring the crime prevention value of LPRs have found effectiveness varied based on a number of factors, including: volume and concentration of LPR deployment, the type of LPR deployed (fixed vs. mobile, general patrol versus specialized unit), location of use, the types of databases connected to LPR and how often they are updated, how officers use LPRs in the field, and agency pursuit and response policies for officers informed about suspects by LPR technology.

Recent technological changes to LPRs may have implications for LPR use and effectiveness. Much of the previous literature is limited to evaluation of mobile LPR units, often mounted in patrol vehicles. The effectiveness of this approach may vary considerably based on how often, and where, the vehicle is driven. Moreover, prior studies have evaluated LPR system that relied on older technology (optical character recognition and infrared technology), limiting license plate capture to reflective metal plates. Modern LPR cameras utilize machine learning to capture a variety of license plates (e.g., temporary paper tags, covered plates), additional license plate information and vehicle characteristics (such as license plate state, vehicle type, manufacturer, and color), and distinguishing vehicle marks (e.g., roof racks, aftermarket wheels, bumper stickers) that could not be captured previously. This additional information may provide investigators with new avenues to investigate and close crimes.

Considering recent developments surrounding LPR technology, the current study seeks to expand understanding of the public safety benefits of LPRs through a multi-site data collection and analysis effort, focusing on fixed-location LPR cameras implemented in several large law enforcement agencies across the United States. Fixed-location cameras can capture license plates and vehicle information from addressed traffic at all hours of the day, providing added investigative benefits.

What We Expect To Learn

Does the implementation of modern LPRs…

- increase arrests for (a) vehicle related offenses or (b) other offenses?
- improve the (a) quality, (b) speed, and (c) close rate of investigations?
- Create a pathway for transparency, open discussion, and engagement with the community? System metrics can be used to answer the following questions: How is the system being used? What data were captured? What searches were being performed? How were the data used?

What Agencies Expect to Gain 928

- 25 Flock LPR units for a one-year trial
- Opportunity to contribute to the advancement of police research nationally
- A custom report on your agency detailing:
- Effect of LPR on crime, arrest, and clearance
- Guidance on more efficacious ways of deploying LPRs
- Being cited in publications as a participant in the research if desired.
- Best practices for development of implementation and operations.

What's Needed From Partner Agencies

Agencies will have an opportunity to participate in a variety of evaluation efforts based on LPR use and staff and data availability (see the Table below). Research activities include:

1. **Provide Preliminary Information** – A survey to understand your use of LPRs, including the number of units, time and locations of when and where LPRs units were installed and expanded, the type of use (e.g., patrol or fixed location), features of the units, and data availability for measuring the intensity and effect of LPR activities.
2. **Provide Existing Fixed-Position LPR Policy (if available)** – Agency should share policy for how LPR is implemented, who has access, pursuit policy, etc.
3. **Provide Agency Data** – Provide agency administrative data, including calls for service, incidents, arrests, and LPR-related activities. Data should cover at least six years.
4. **Evaluation** – Participate in evaluation efforts including interviews, focus groups, and data collection efforts.

Type of Agency	Number of Agencies	Expected Role
Tier 1	4 - 6	• Provide dispatch, incident, and arrest data • Provide vehicle location data • Provide LPR data (number of scans and alerts) • Access to information about investigative use of ALPR data • Interviews/focus groups with LPR users • Involvement in LPR placement
Tier 2	40 to 50	• Provide dispatch, incident, and arrest data • Provide LPR data (number of scans and alerts)
Tier 3[1]	40+	• Provide LPR data (number of scans and alerts)

1 For tier 3 involvement, agencies will have the option to participate in the study anonymously.

Research Team

The research will be led by Drs. Travis Taniguchi (Research Director) and Hannah Wu (Senior Research Associate) from the National Police Foundation, an independent, non-profit, non-partisan research organization

Contact

Travis Taniguchi, PhD
NPF Research Director
ttaniguchi@policefoundation.org



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS Administrator's Manual

Version 2.14

Updated 7/16/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.2.1 Getting Started in PAGIS 8

2.3 The PAGIS Navigation Buttons 9

2.3.1 Camera Control Buttons 9

2.3.2 GPS Indicators 10

2.3.3 Camera Firmware Update (Restricted Users) 10

2.3.4 Day/Night Mode 10

2.4 Begin Shift 11

2.4.1 Sync via USB Thumb drive (or Local Source) 11

2.4.2 Sync via Wireless Network 11

2.4.3 PAGIS Auto-Sync Settings 11

2.4.4 Begin Shift – Additional Information 11

2.5 End Shift 11

2.5.1 Sync to BOSS 11

2.6 Cam Mode Button 12

2.6.1 Camera Modes 12

2.7 Taking a Picture 12

2.8 Search Entry Screen 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits 13

2.8.2.1 Searching for a Match 14

2.8.3 Wild Card Symbols 14

2.8.4 Manually Adding a Plate to PAGIS 15

2.8.4.1 ADD VLP Query 15

2.8.4.2 ADD VRM Report Screen 15

2.9 The Review Screen 16

2.9.1 Summary Review Section 16

2.9.2 Review Navigation Buttons 16

2.9.3 Reads 17

2.9.3.1 Reads Result Screen Navigation Buttons 17

2.9.3.2 Interactive Buttons – Reads Screen 17

2.9.4 Hits 18

2.9.4.1 Hit Screen Attributes 18

2.9.4.2 Hit Screen Function Buttons 19

2.9.4.3 Interactive Buttons – Hits Screen 19

2.9.4.4 Set Disposition – Additional Detail 19

2.9.4.5 Add Intel – Additional Detail 20

2.9.5 Misreads 20

2.9.5.1 Marking a Record as a Misread: 21

2.9.6 Audits 22

2.9.7 Targets 22

2.9.7.1 The Targets Screen 23

2.9.7.2 Targets Screen Navigation Buttons 23

2.9.8 Databases 24

2.9.8.1 Databases Screen Functions 24

2.9.8.2 Databases Screen Navigation Buttons 24

2.9.8.3 Databases Edit- “Manual Reports” 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization Types 26

3.1.1.1 Synchronization to Disk (Local Storage) 27

3.1.1.2 Synchronization with BOSS 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 28

3.1.2 Global Sync Options 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

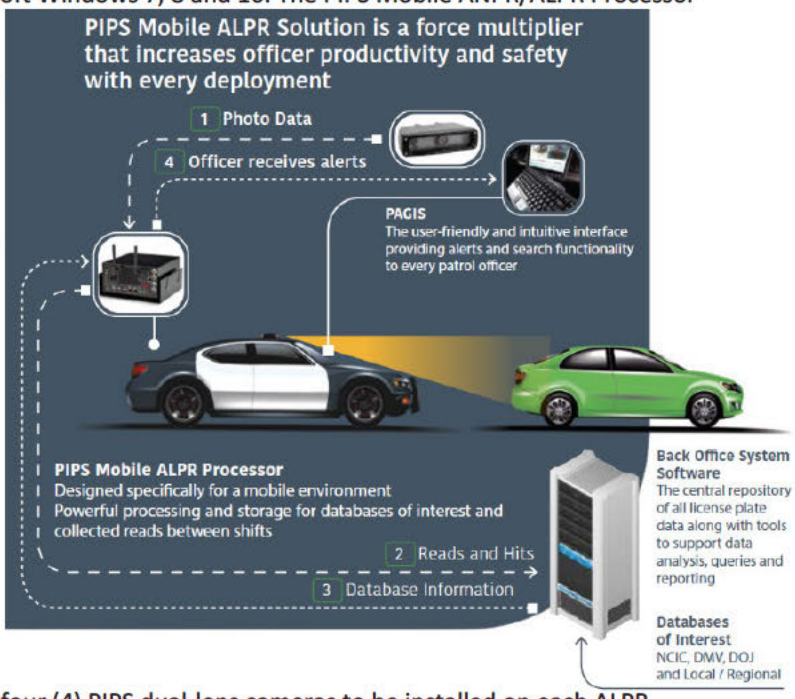
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

934

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

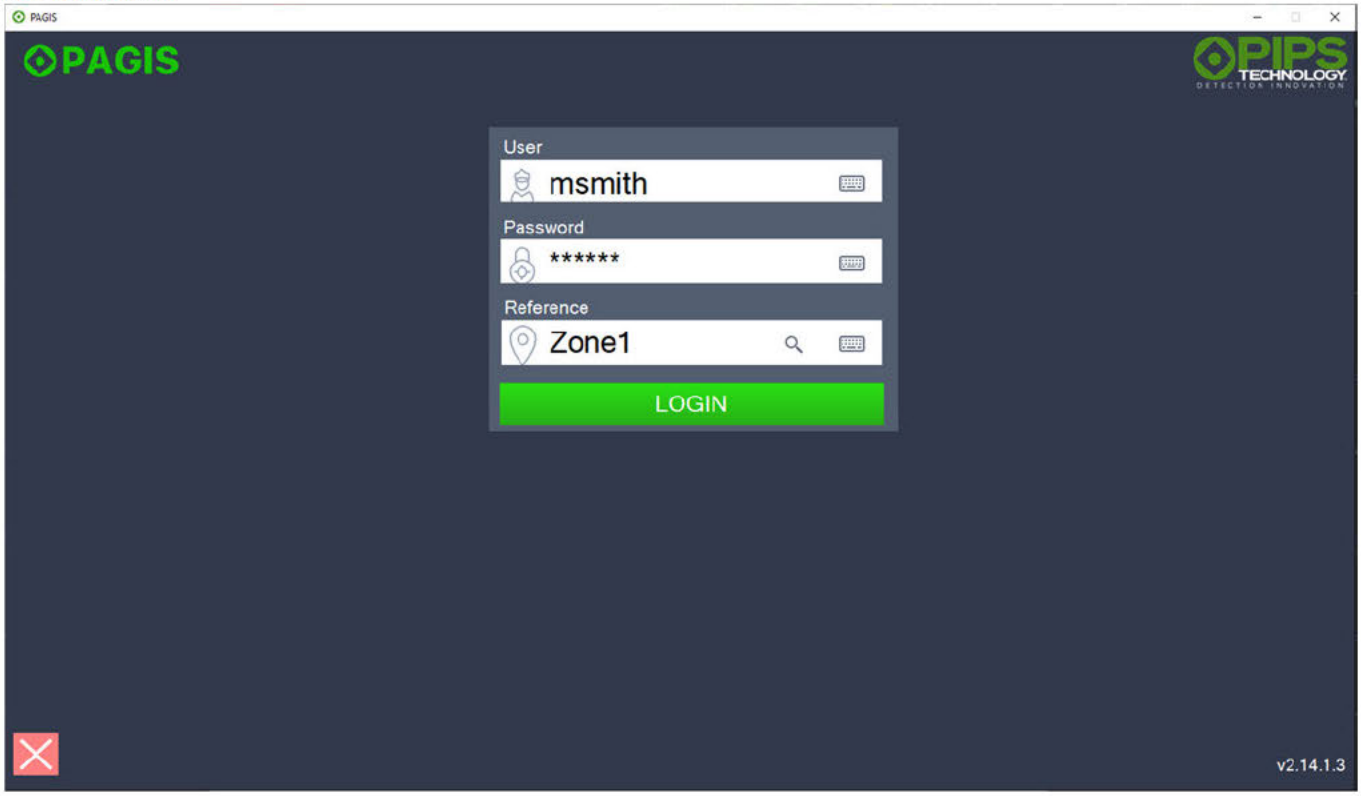
Section 5: Additional Information and Troubleshooting Tips

Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

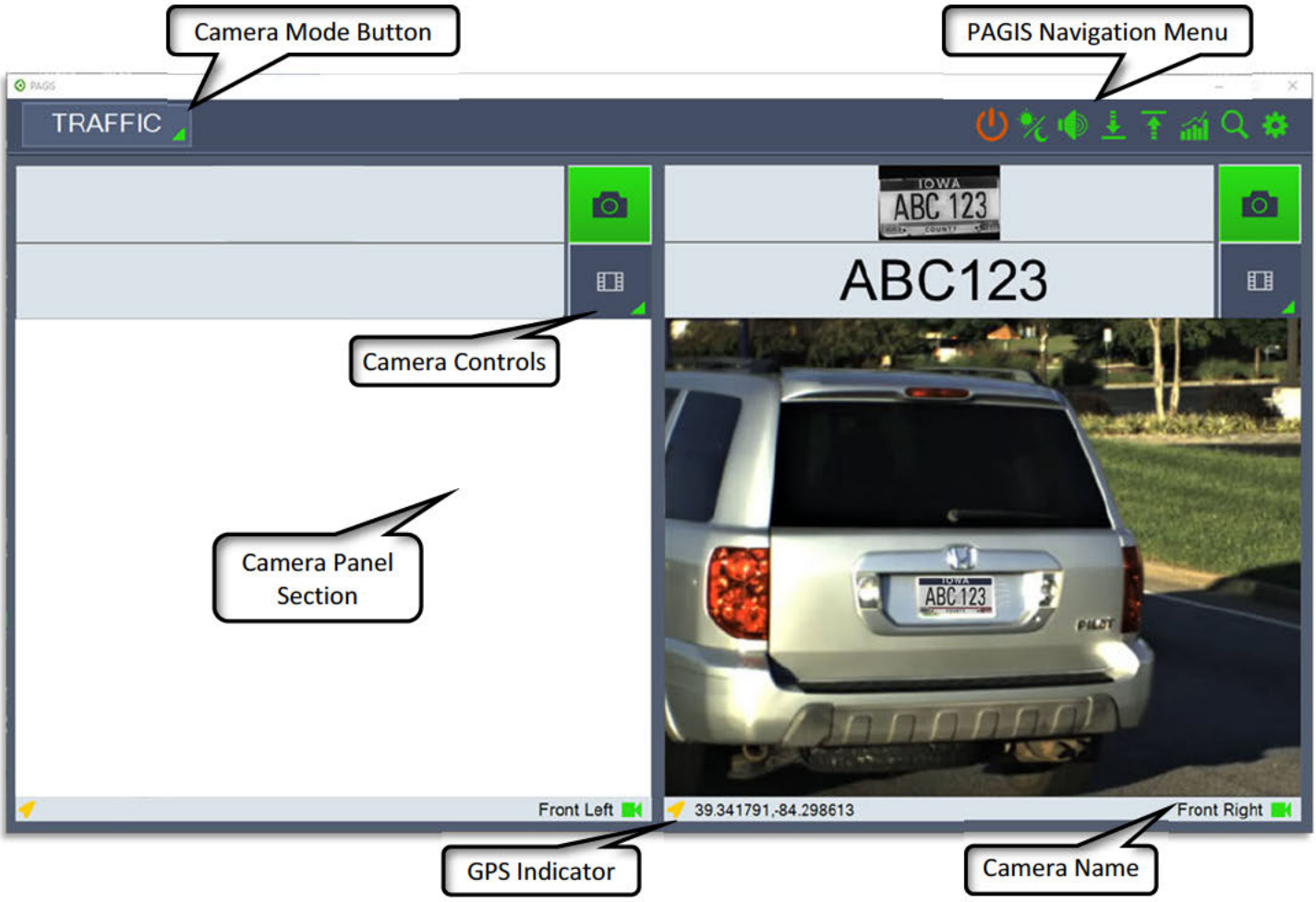
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

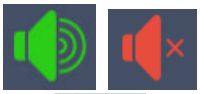
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

938

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

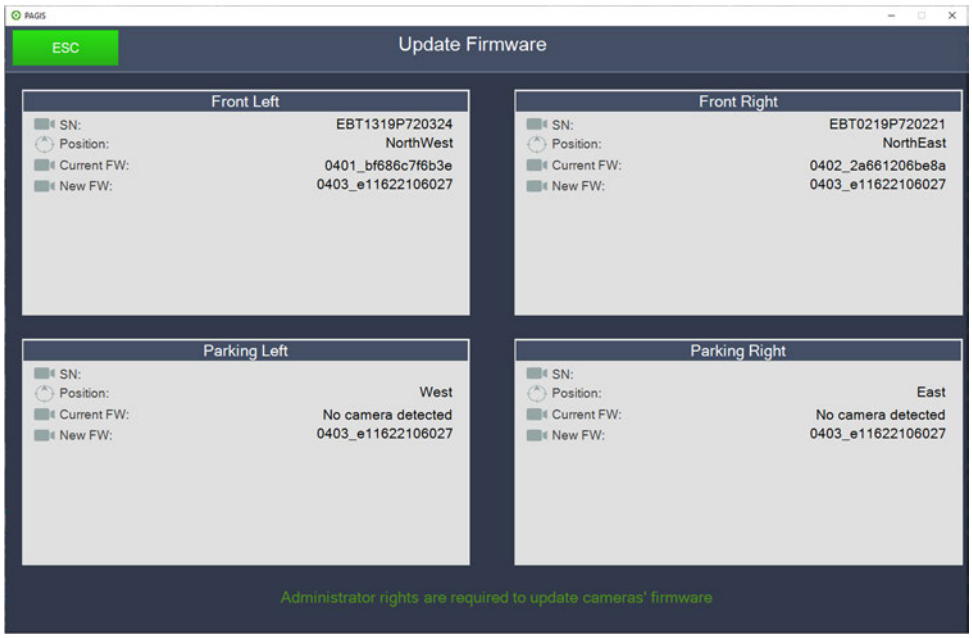
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

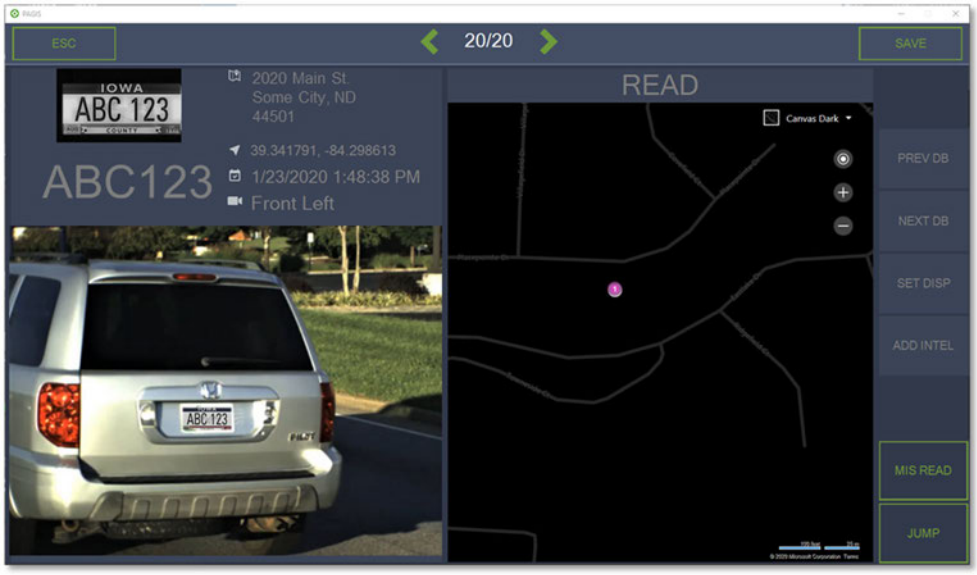


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

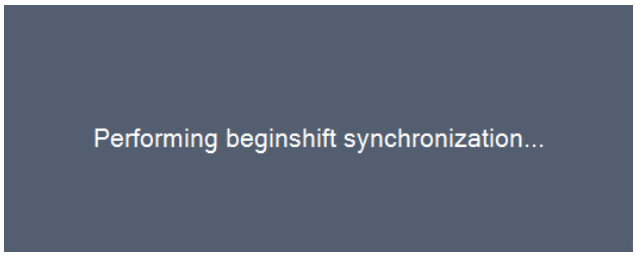
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

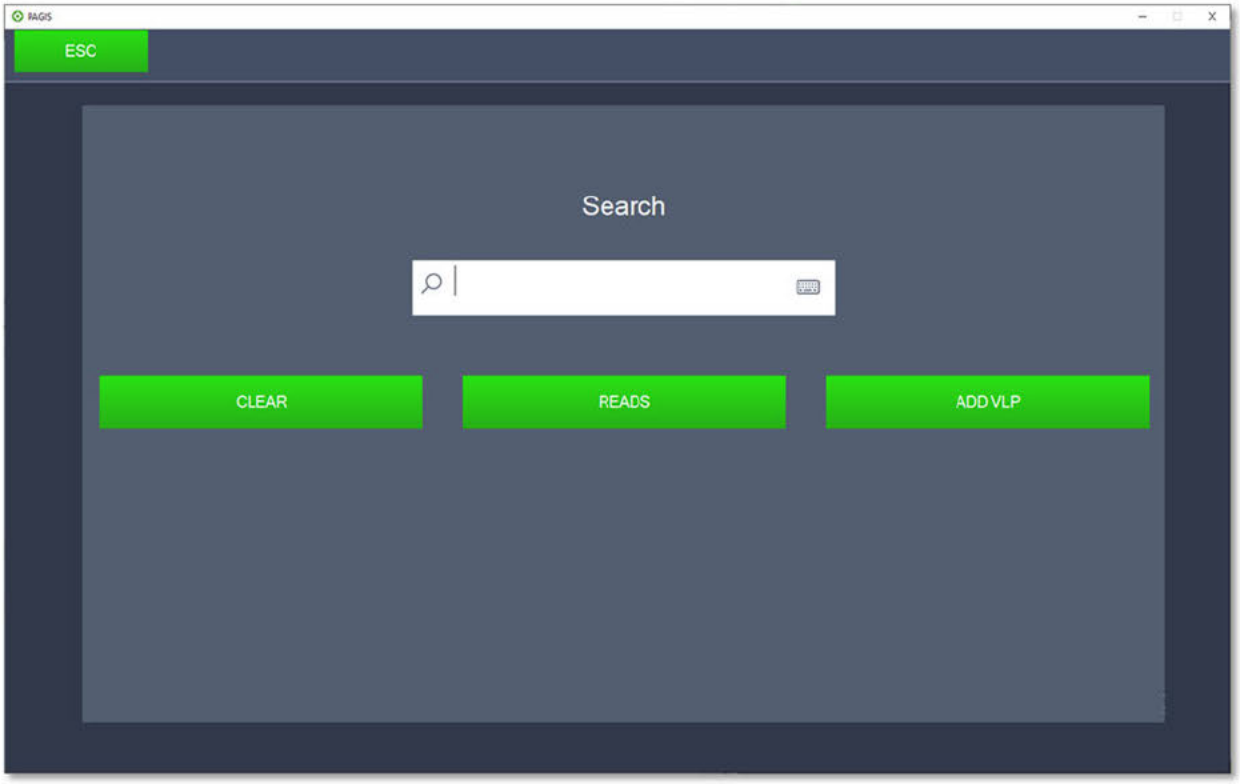
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

942

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

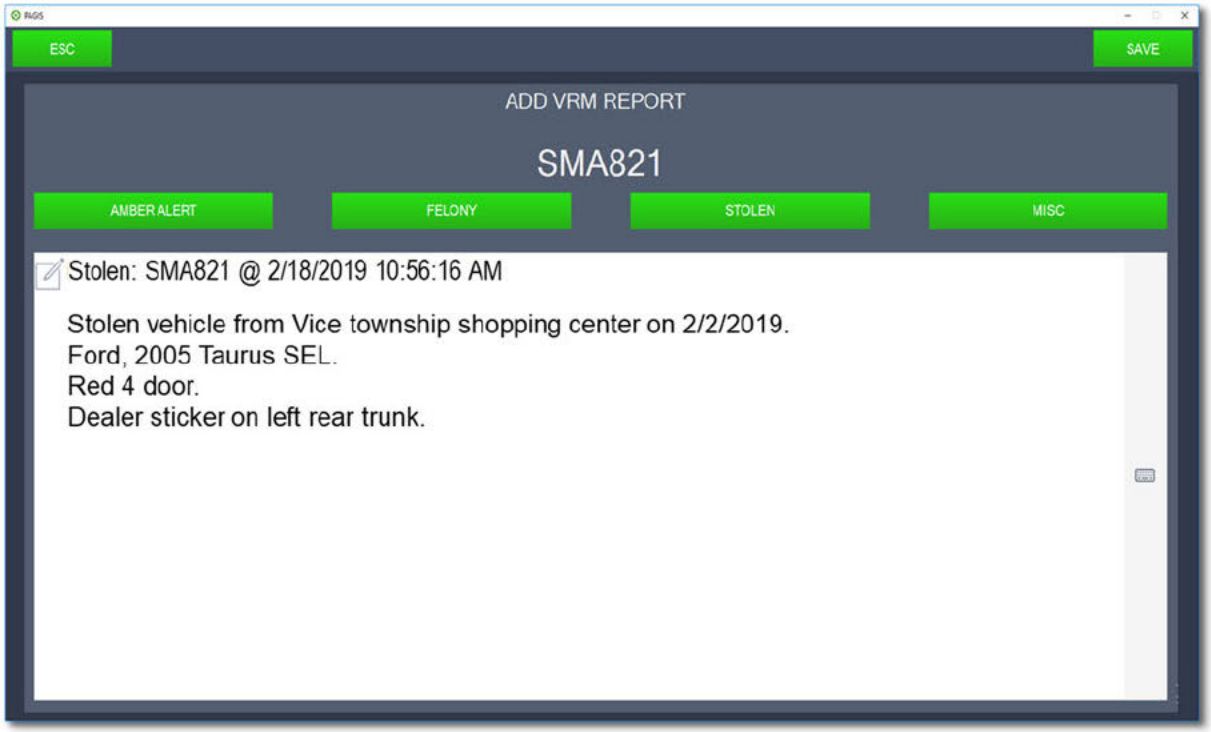
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

944

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

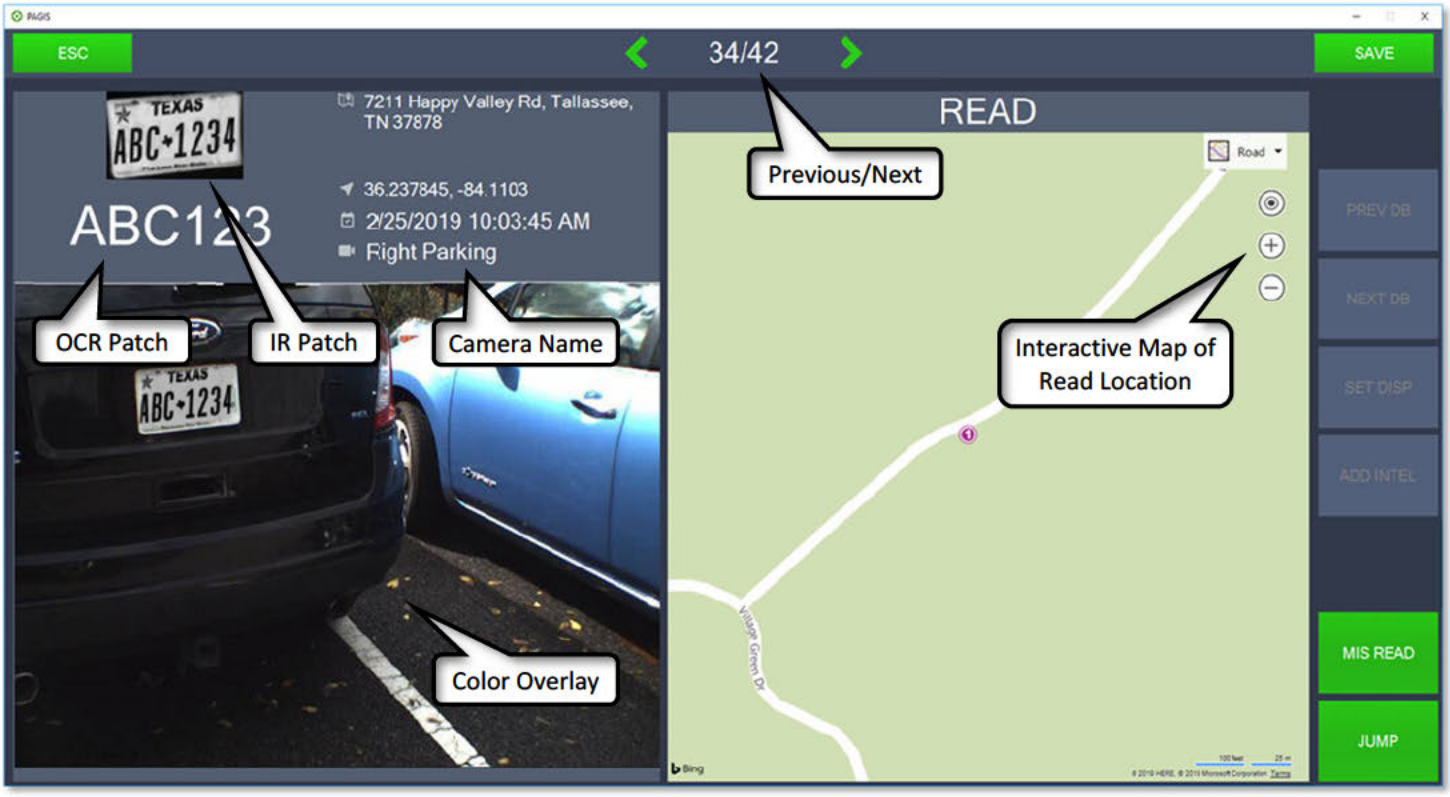
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

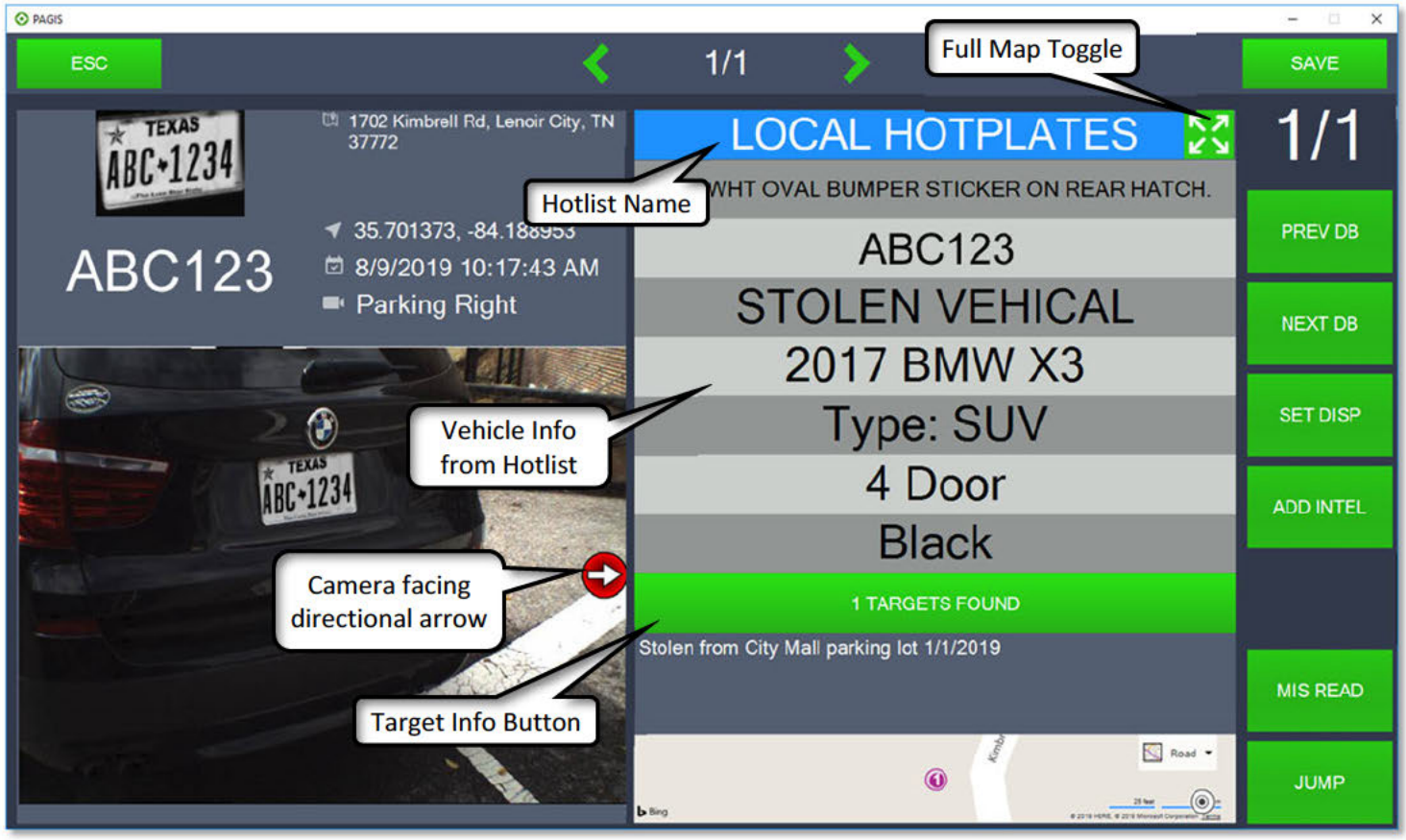
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.
IR Patch Image: A thumbnail image of the license plate from the IR camera.
OCR Text: The character string the OCR engine generated from the current plate.
GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).
Date and Timestamp: The date and time when the read/hit was captured.
Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)
Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).
Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.
Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.
Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.
Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

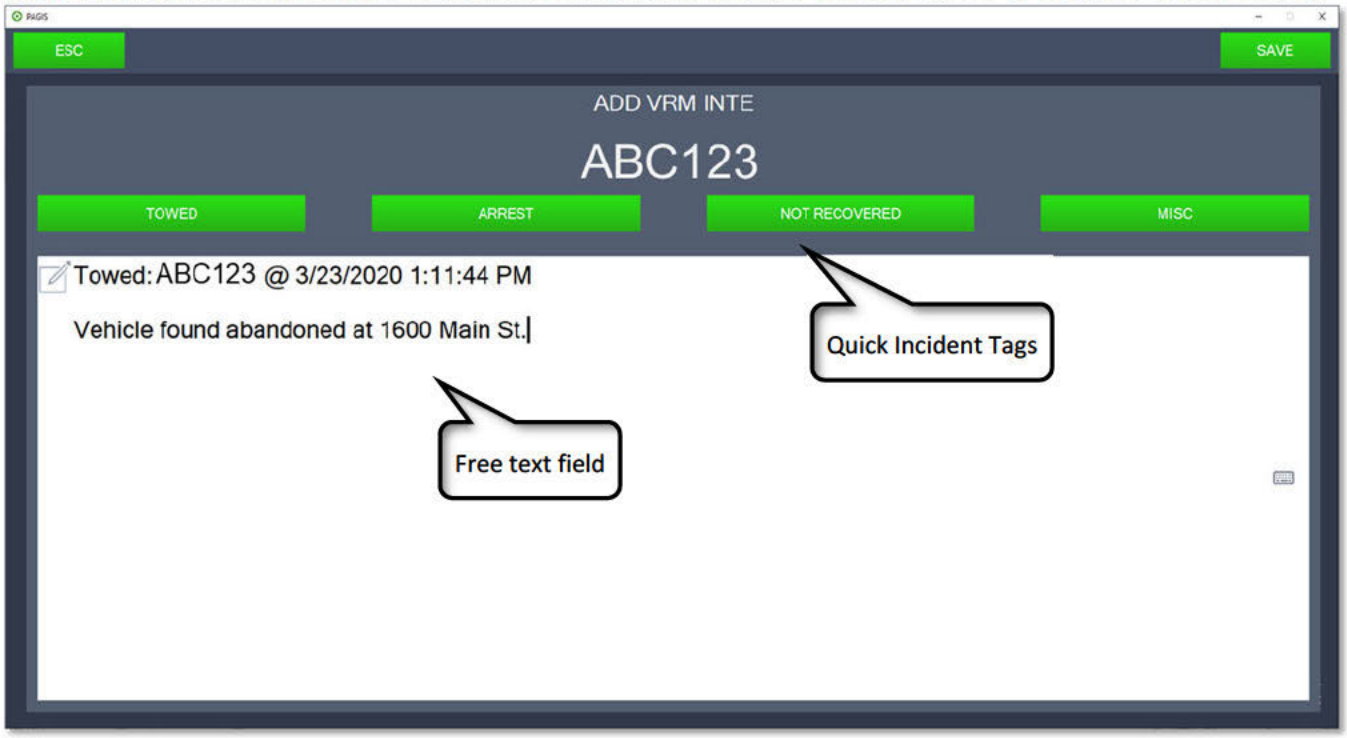


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

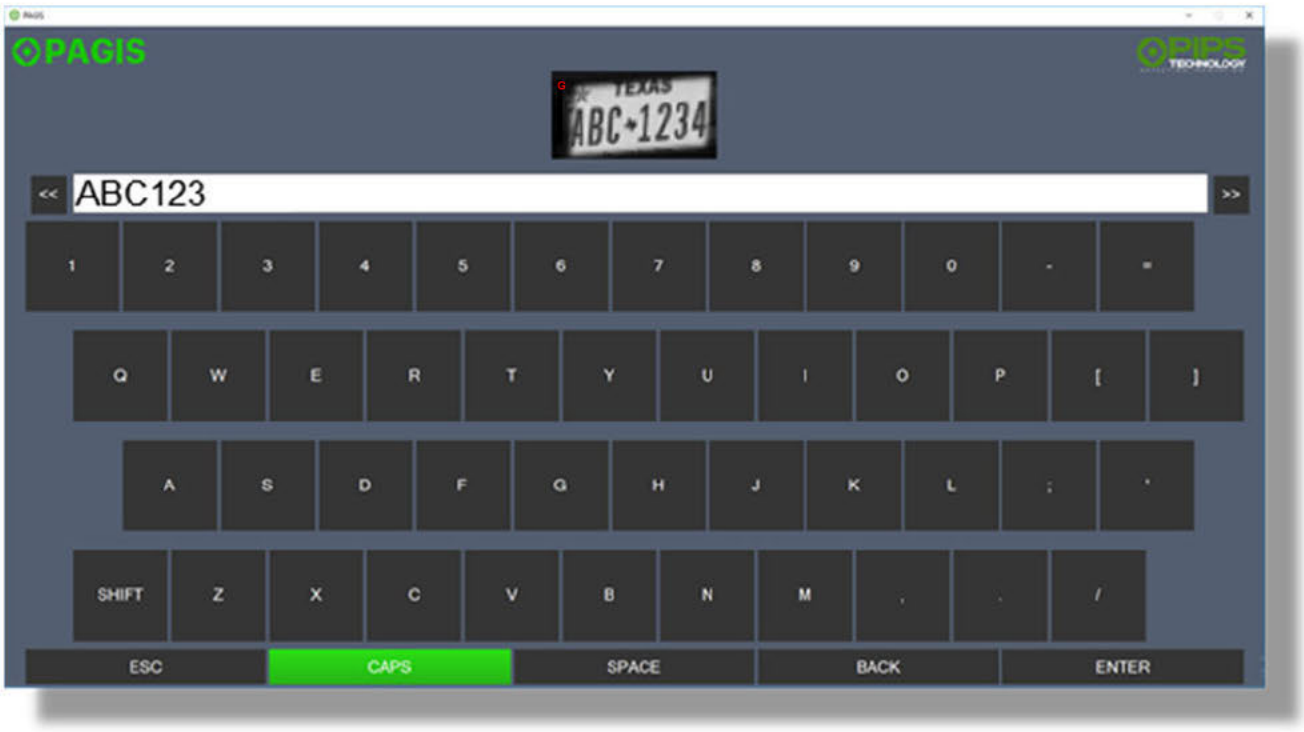
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

Updating the Read/Hit OCR Patch:

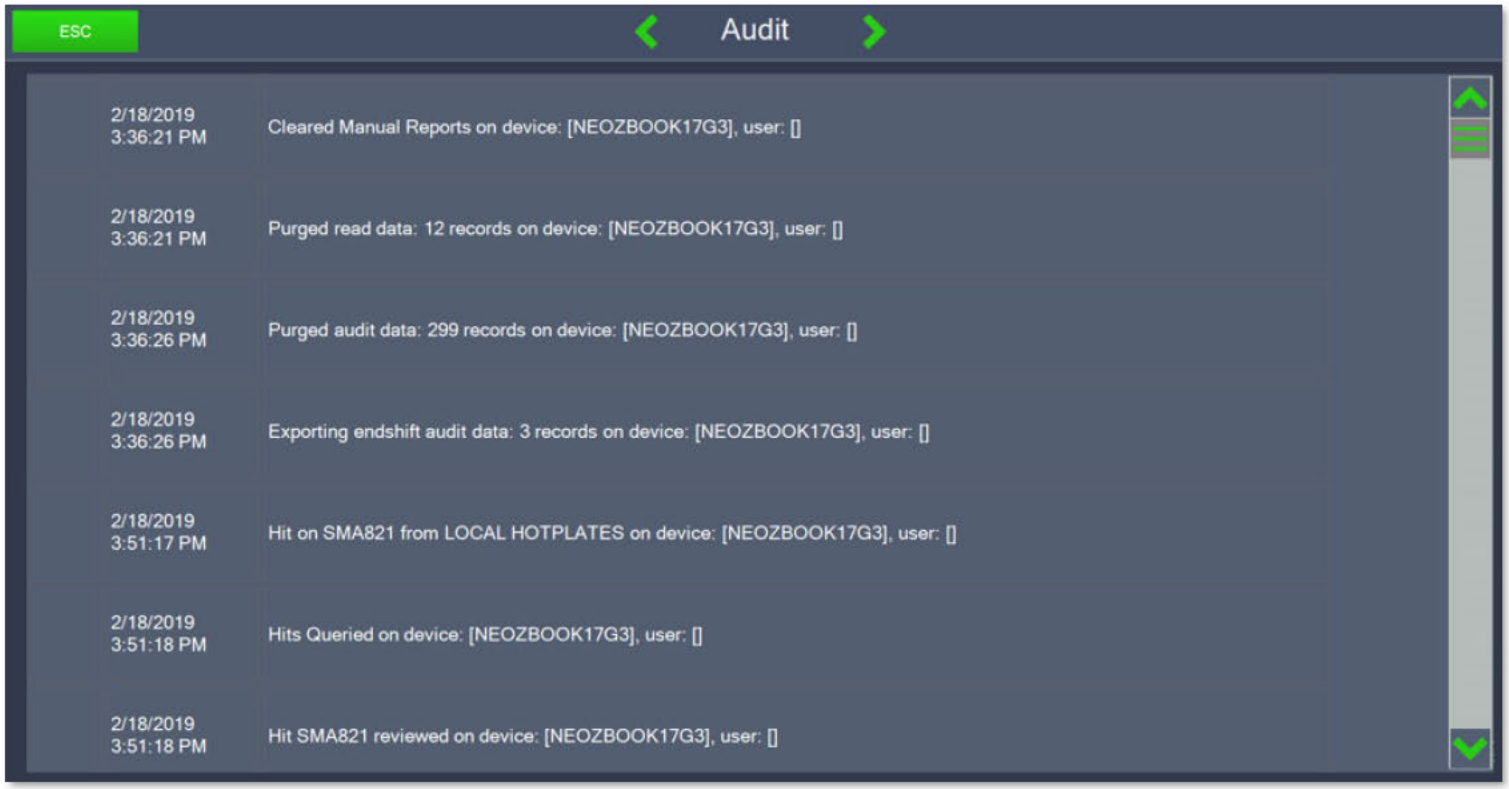
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

950

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



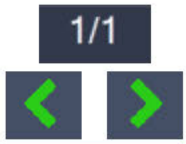
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

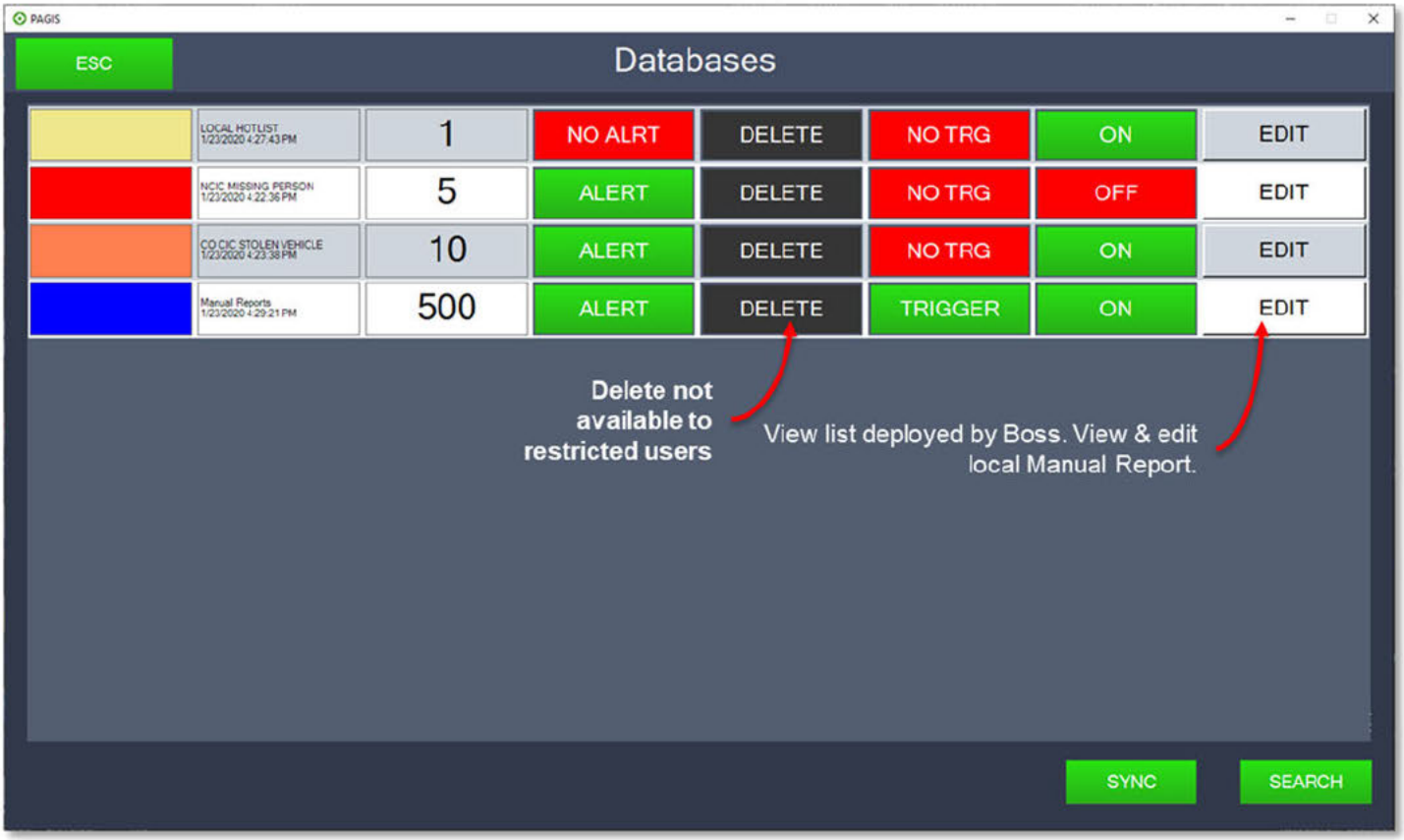


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

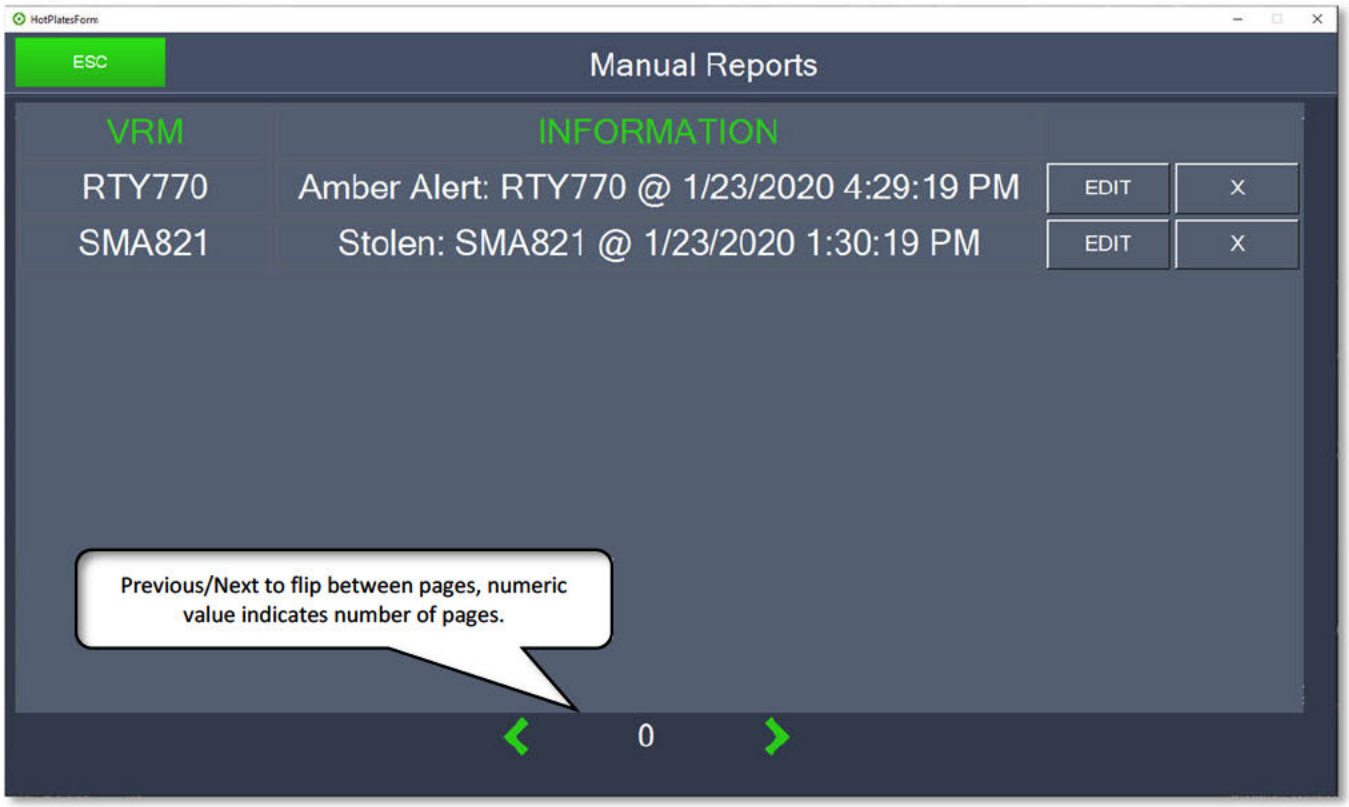
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



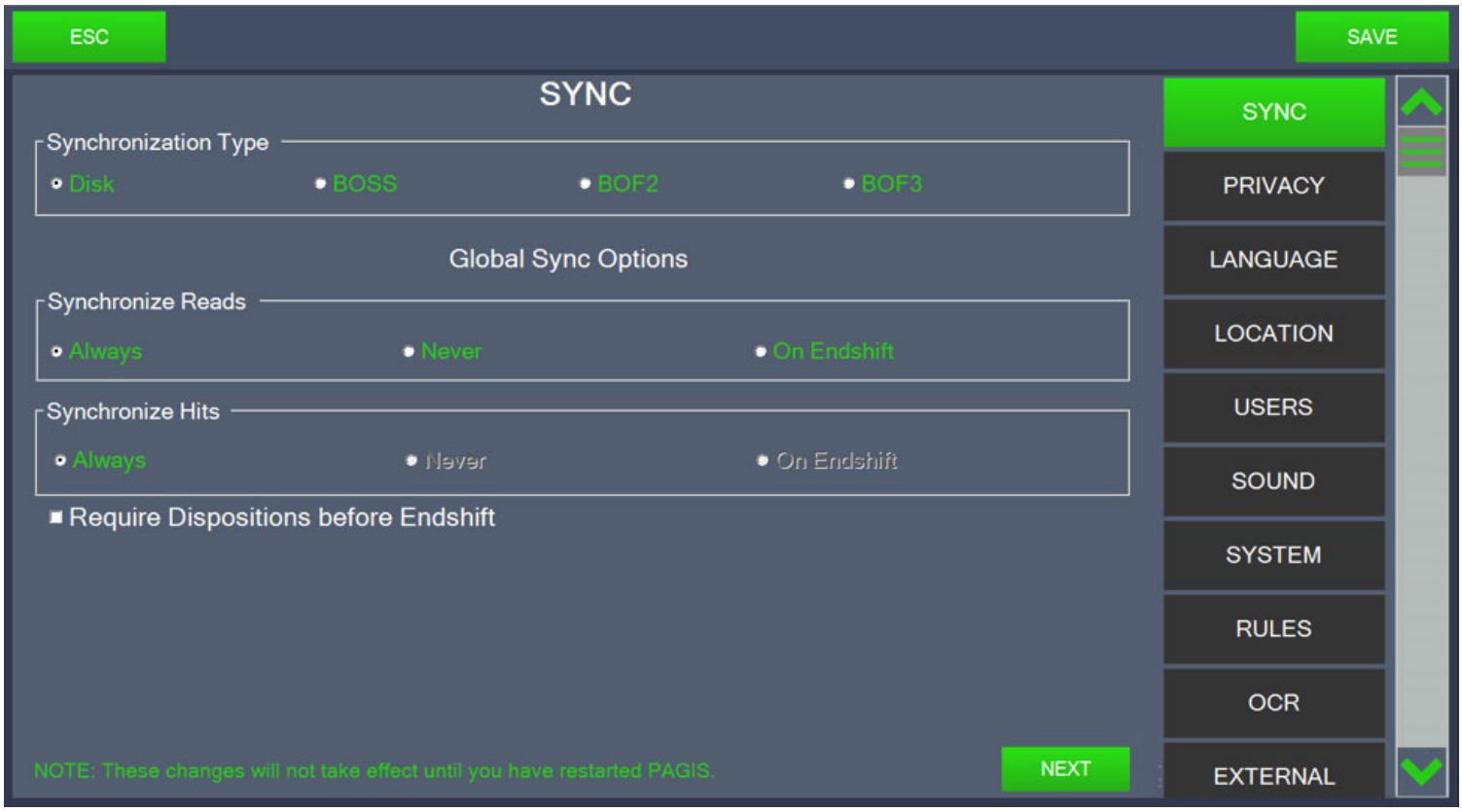
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

955

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

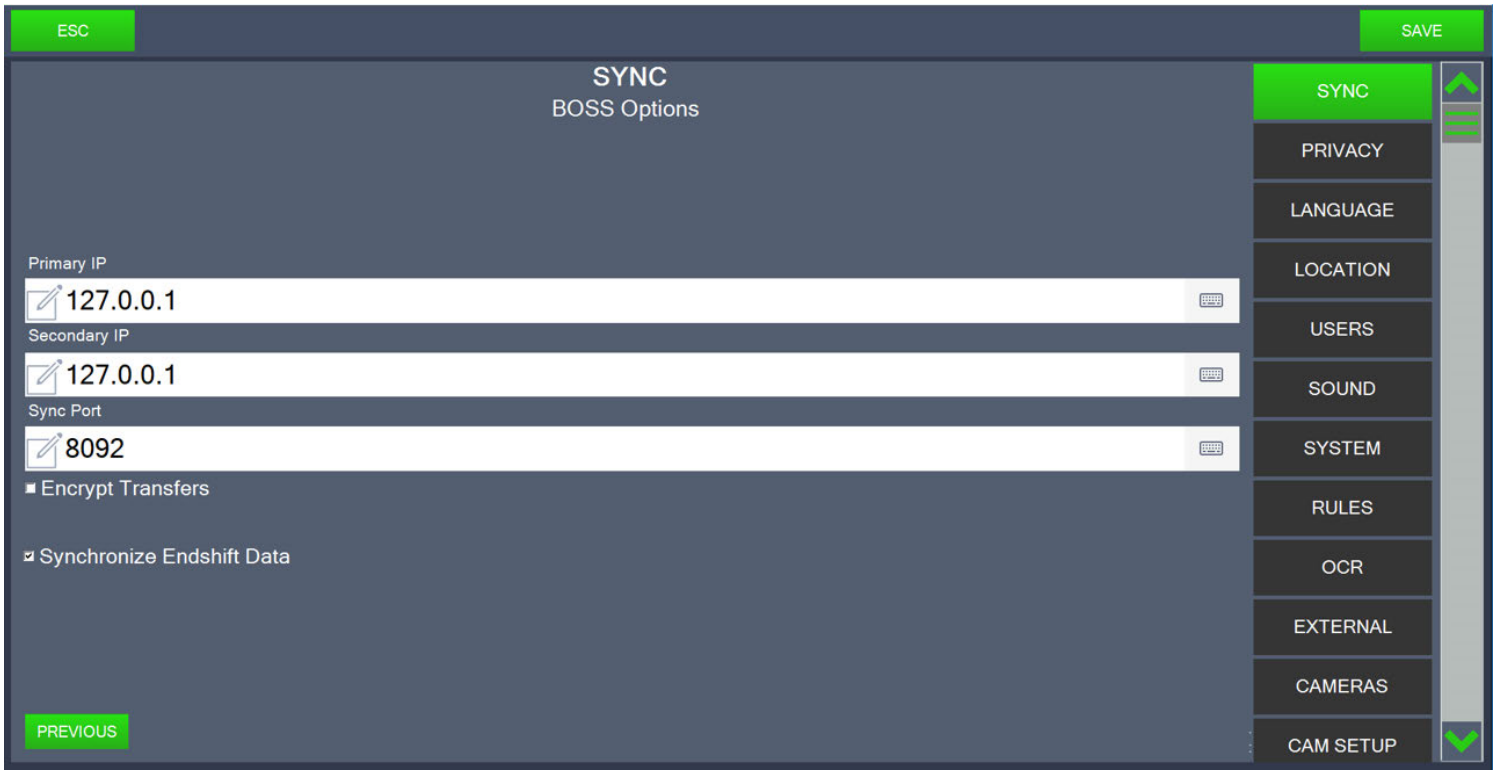


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

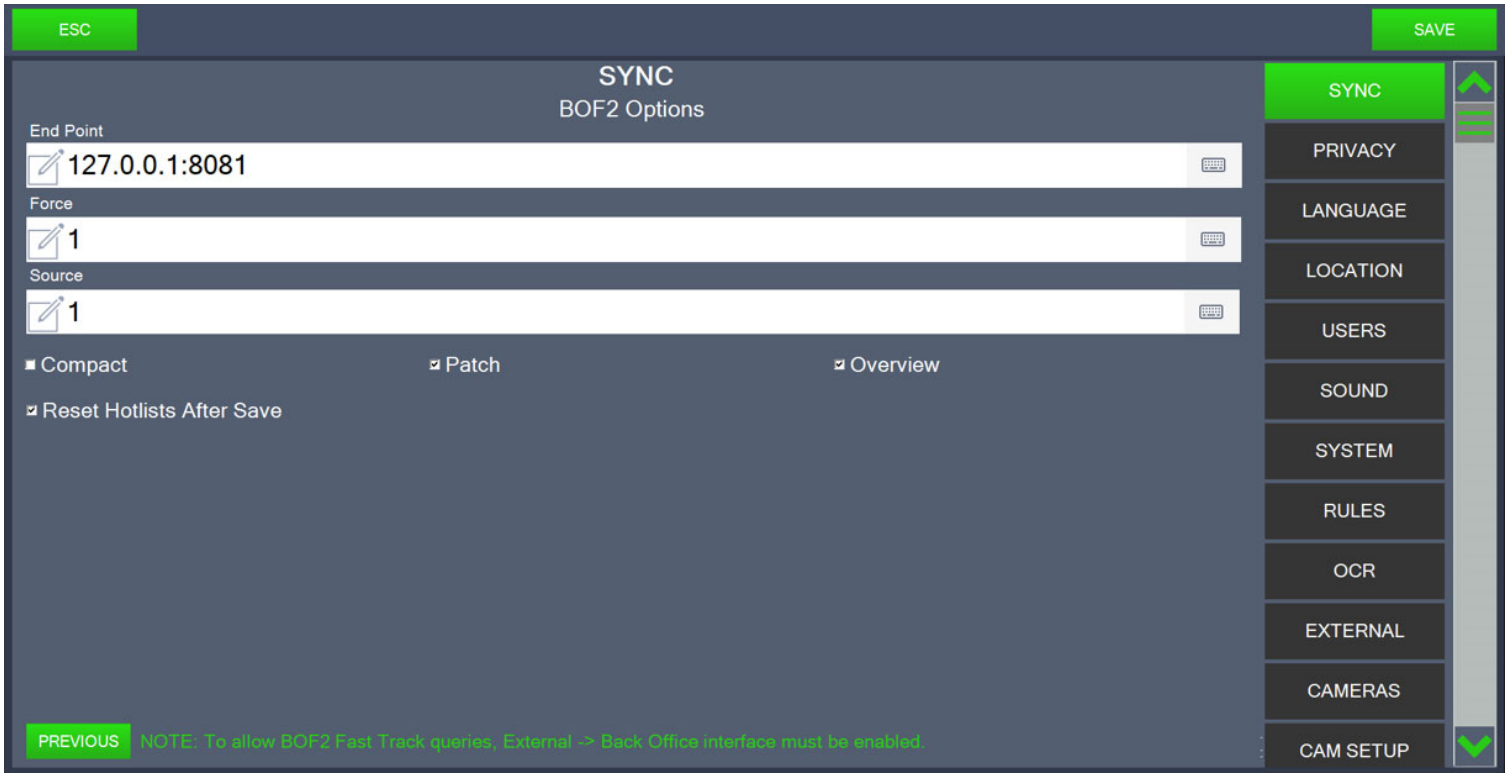
- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:
To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)
NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the PIPS BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.

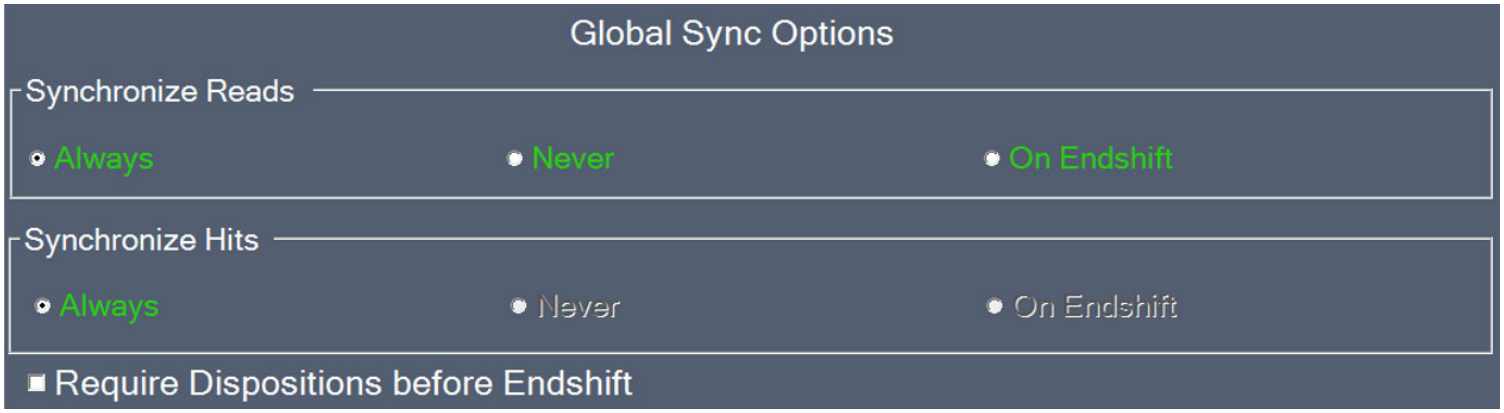


- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

957

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



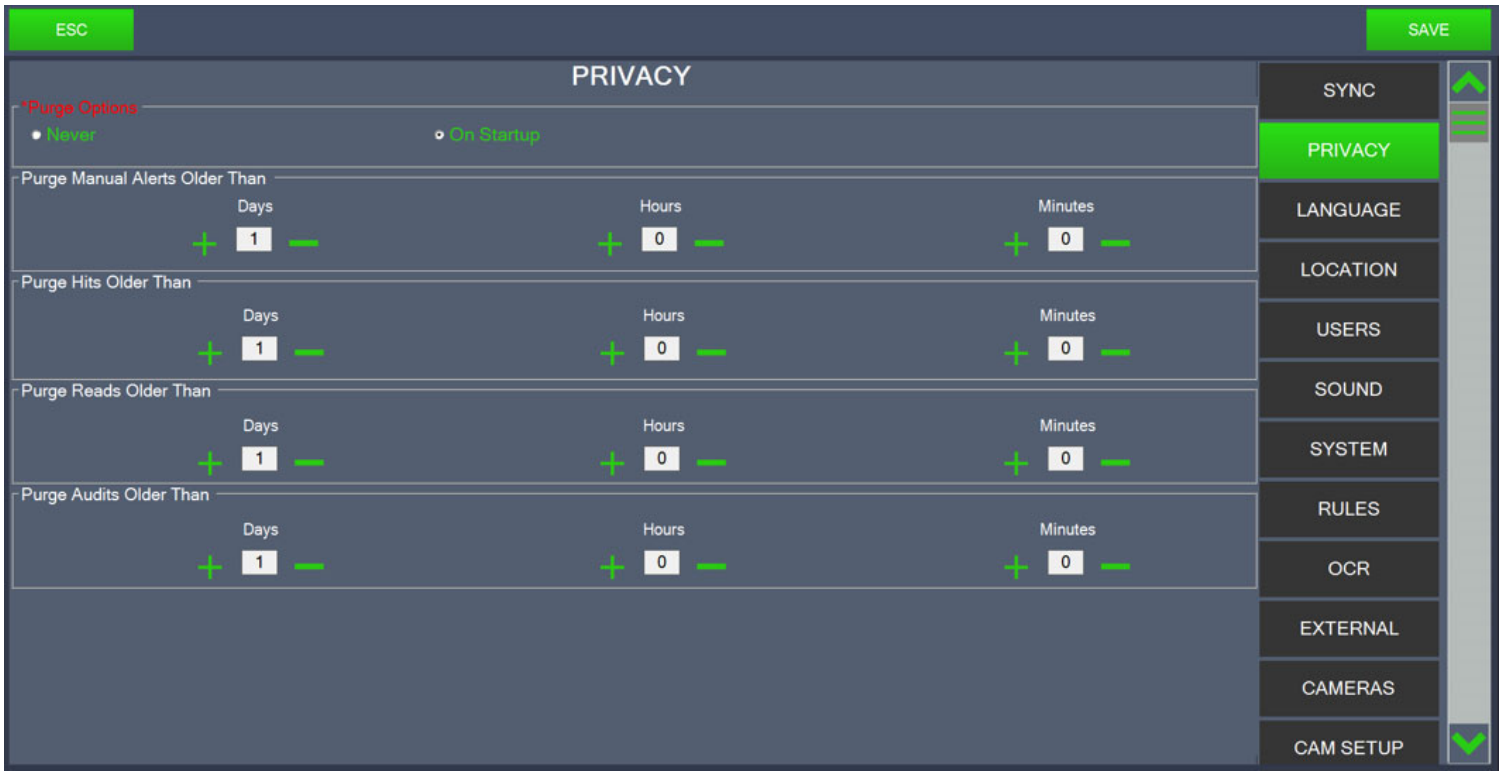
NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

958

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

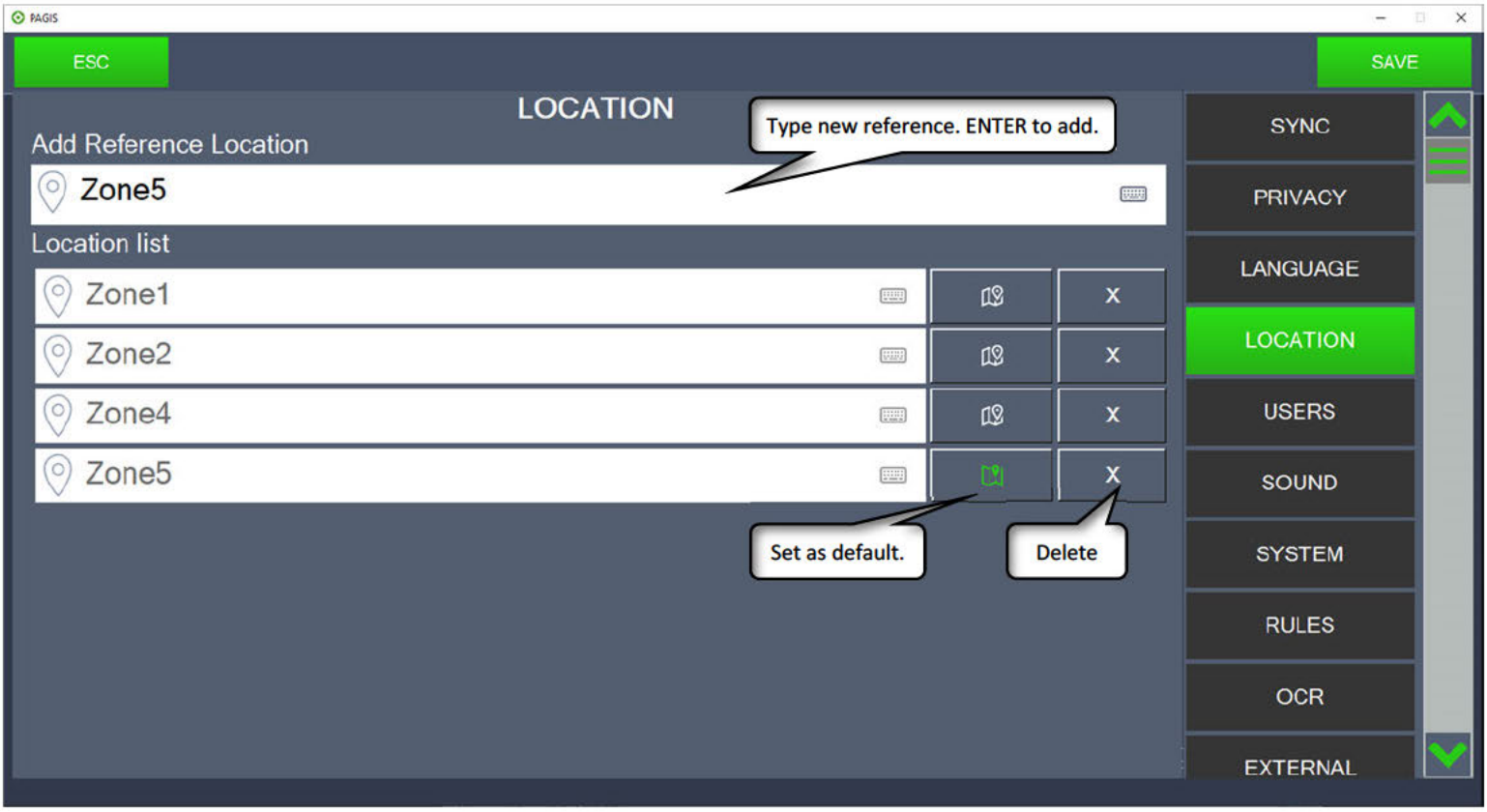
3.3 Language

959

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

3.4 Location

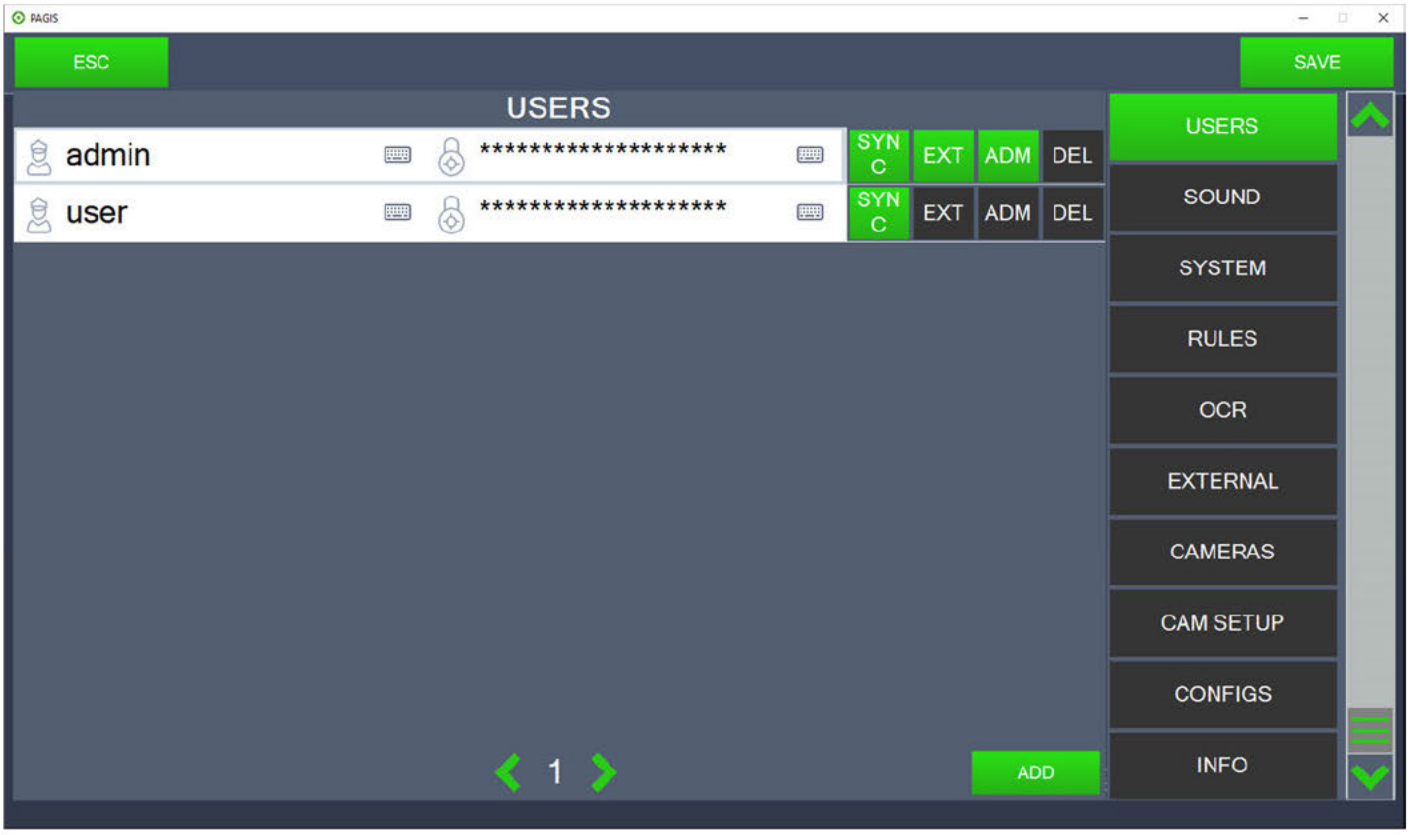
Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users

960

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

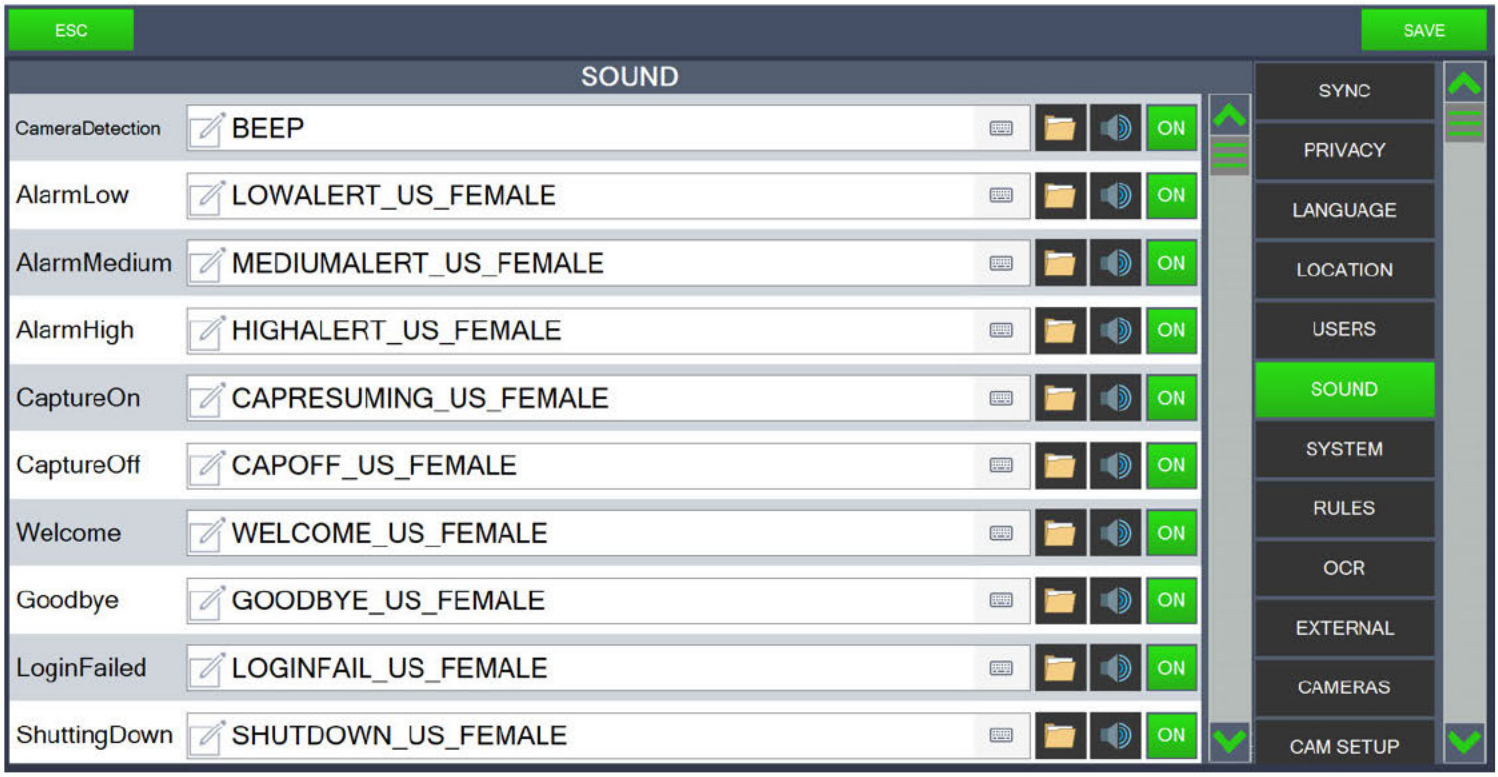
DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound

961

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



Shows the status of that sound. Click to turn each sound Off.

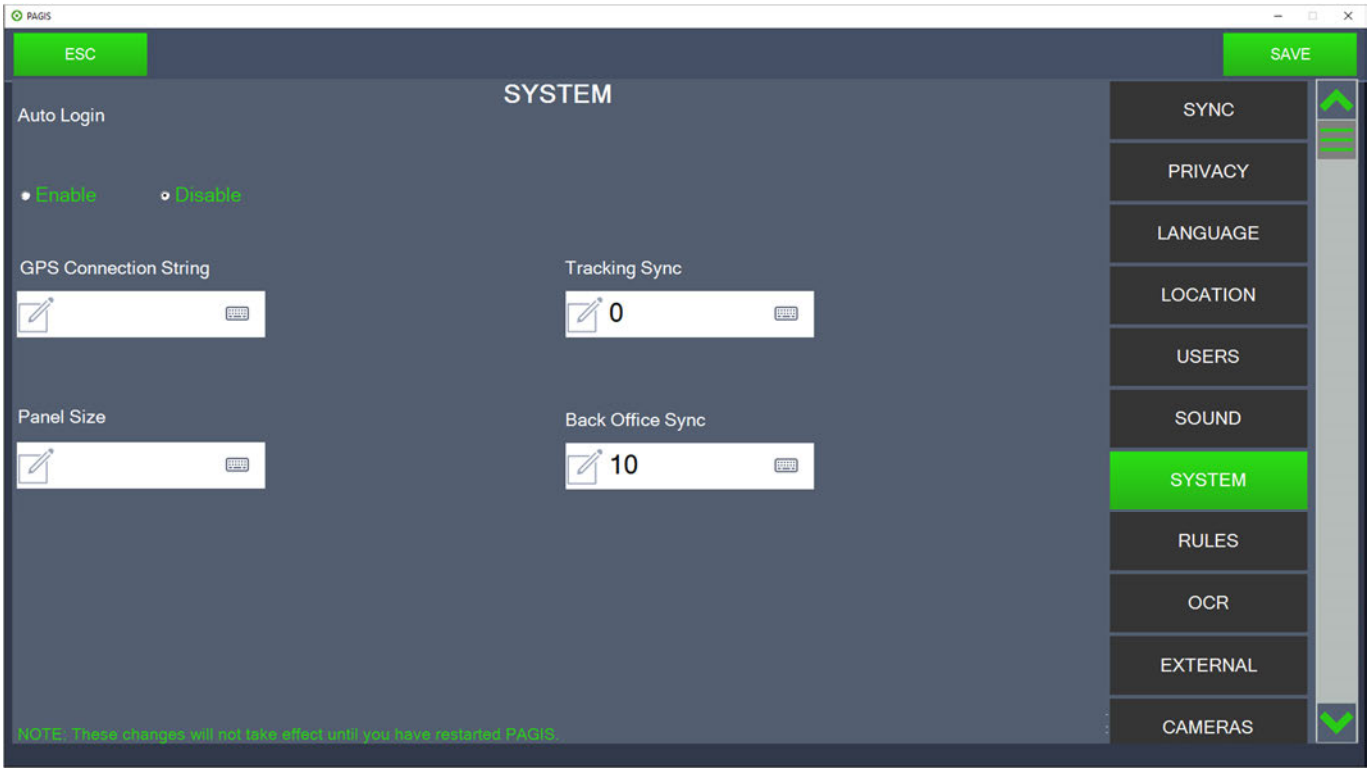


Shows the status of that sound. Click to turn each sound On.

3.7 System

962

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).

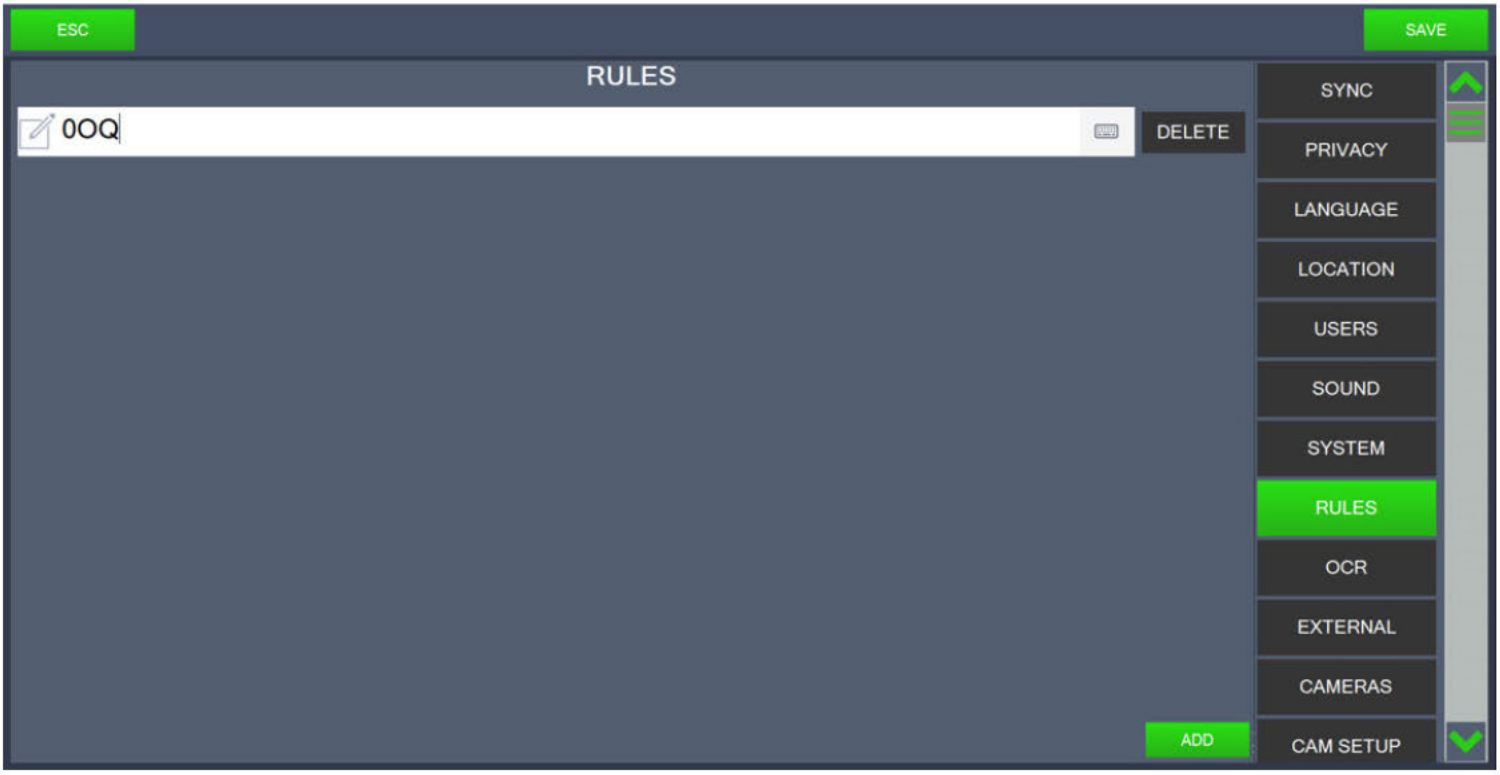


- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of PIPS Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

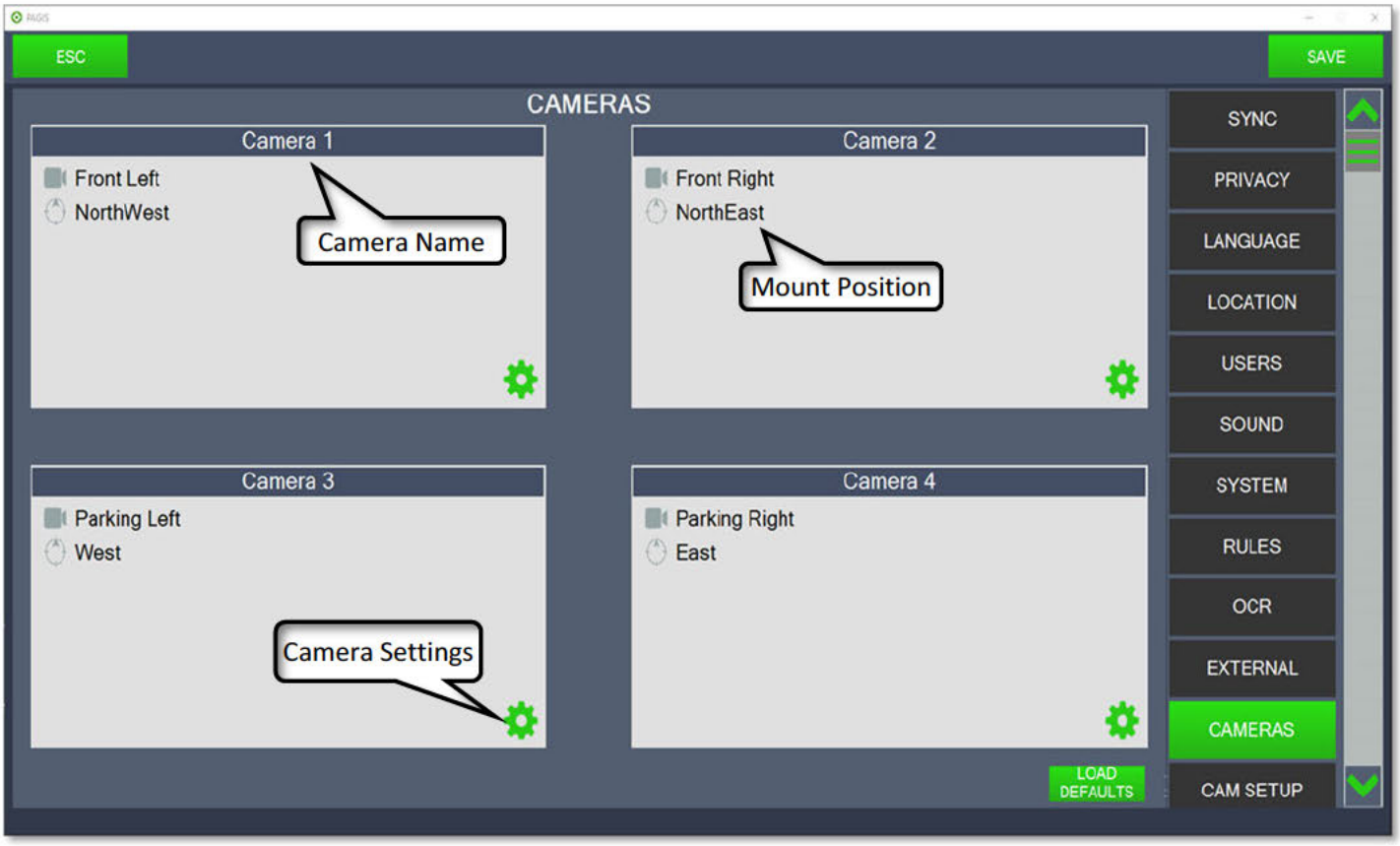
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

3.11 Cameras

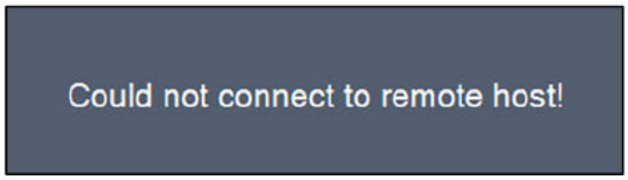
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

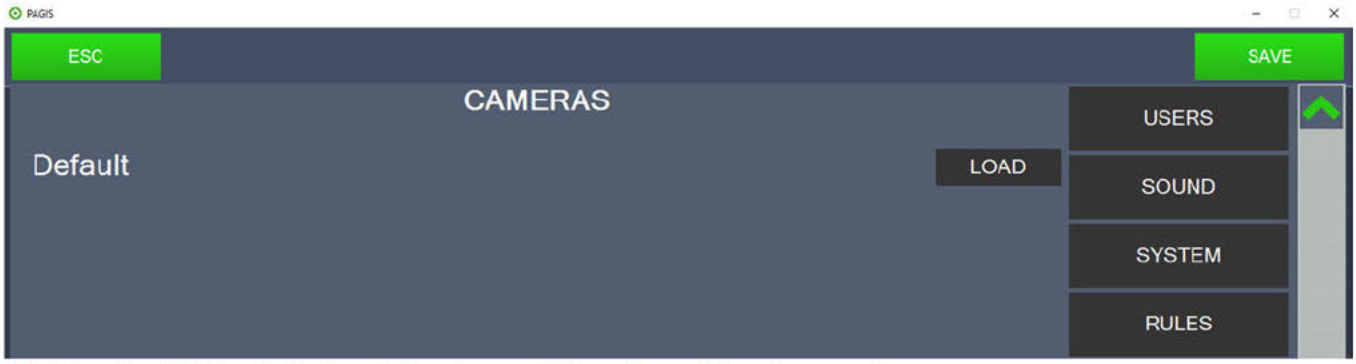
The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact PIPS Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button LOAD DEFAULTS. This manual will start with Load Defaults.

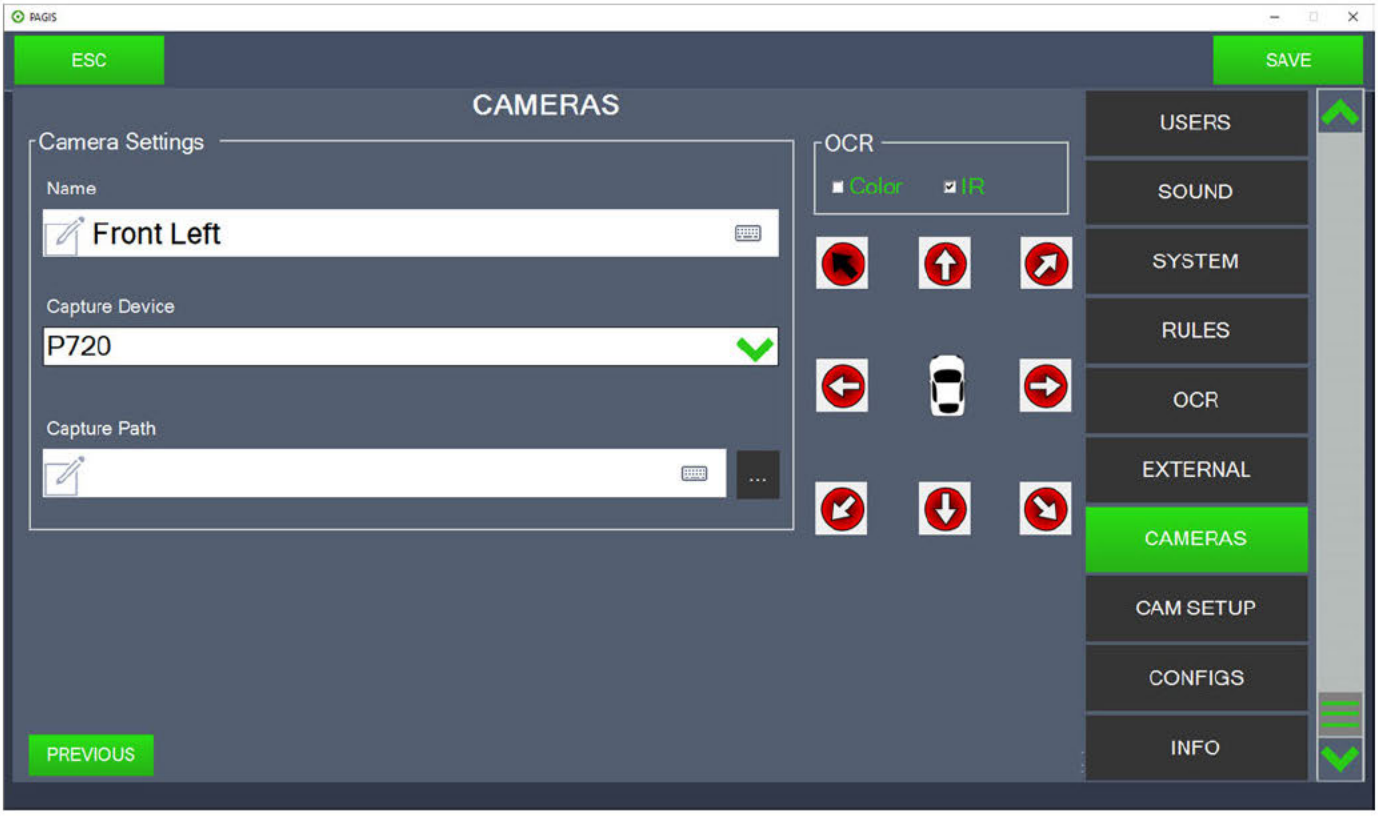
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button LOAD
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

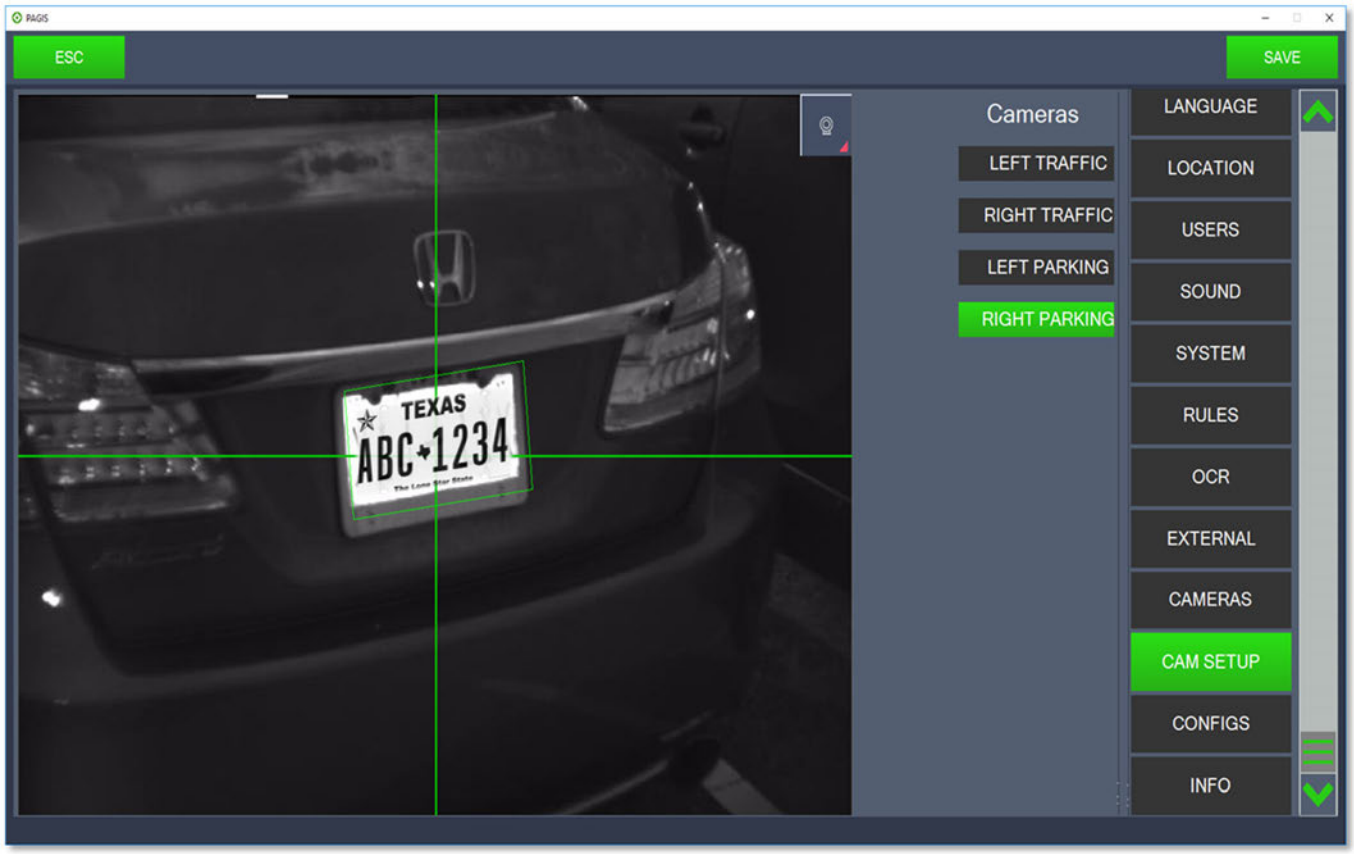
This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.



1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

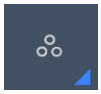
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.

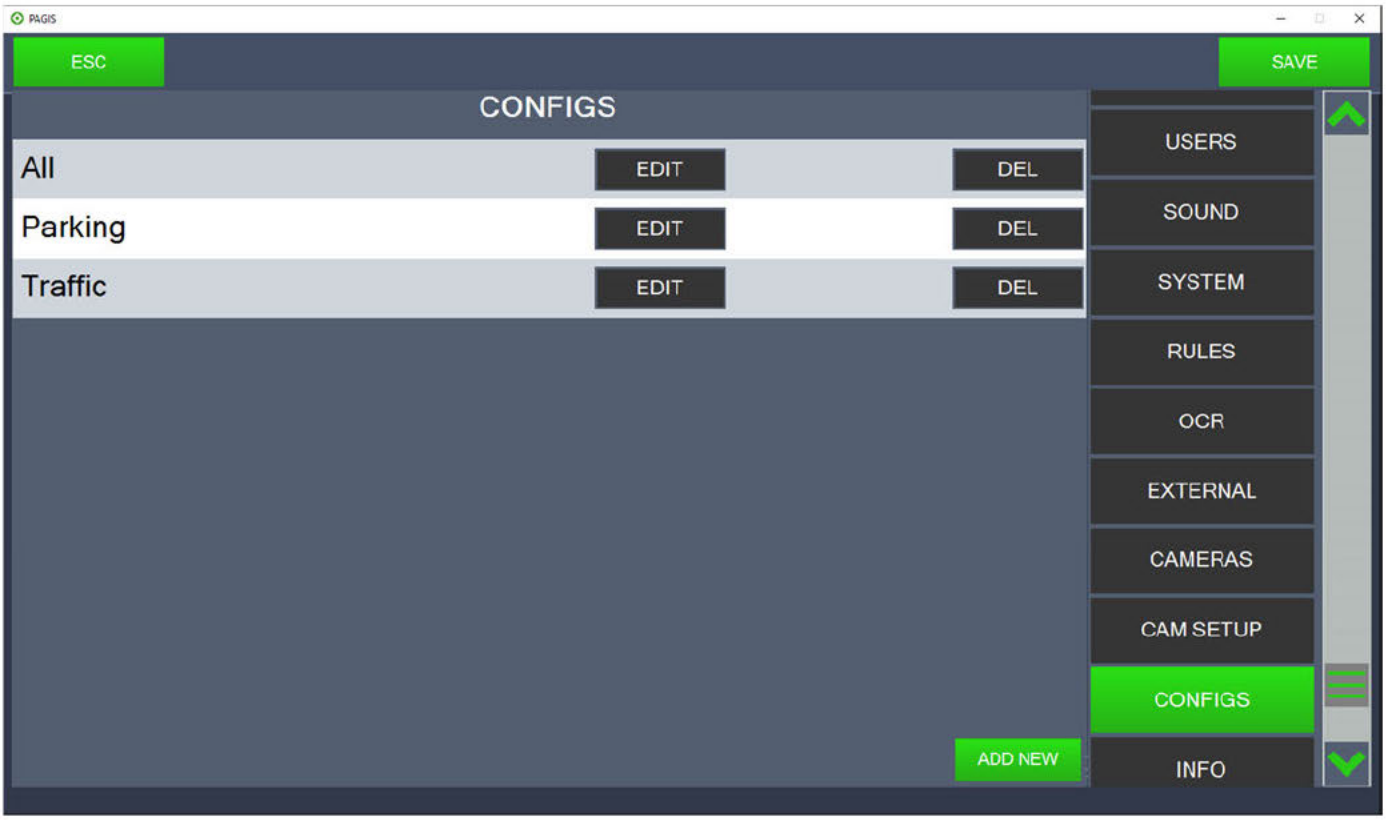


IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button

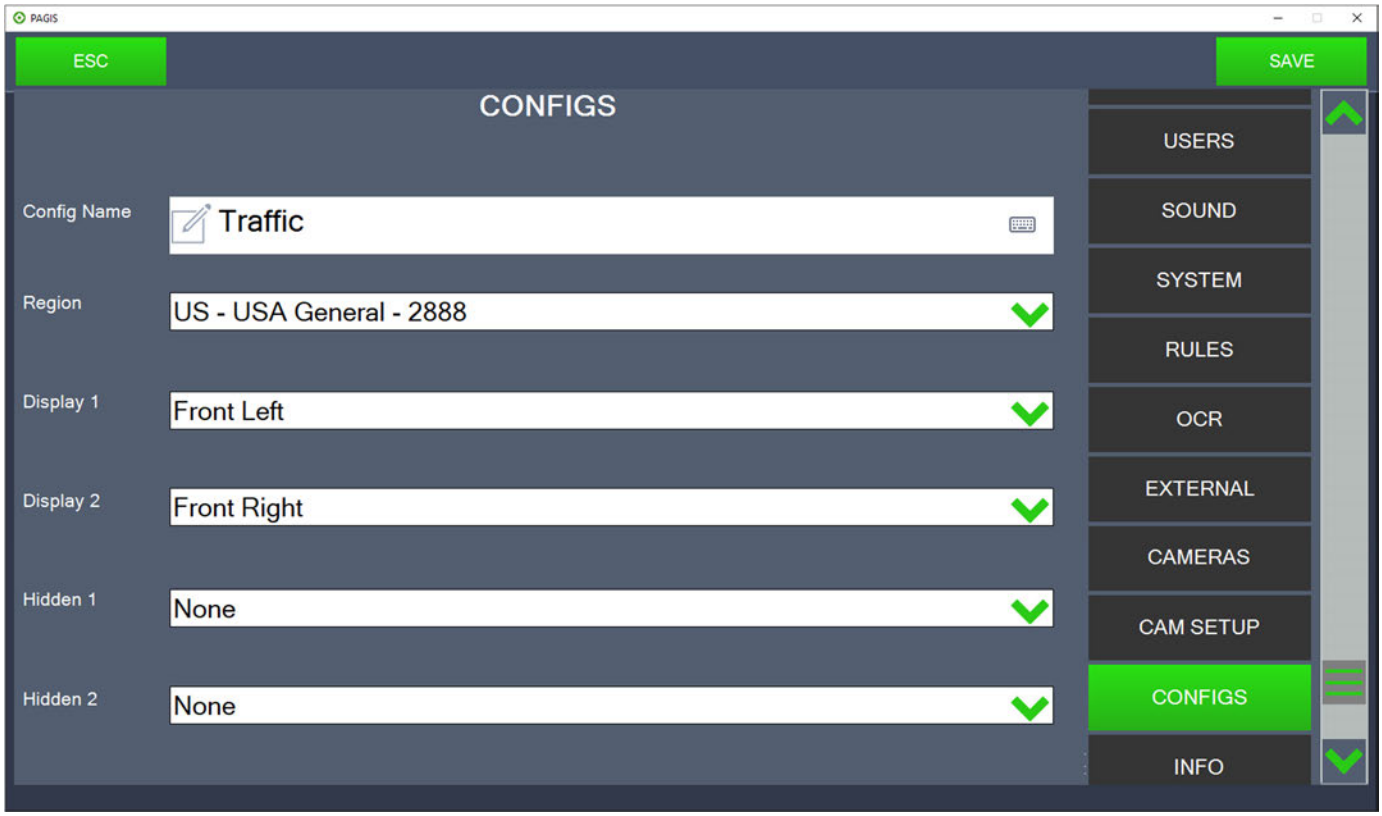


To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.

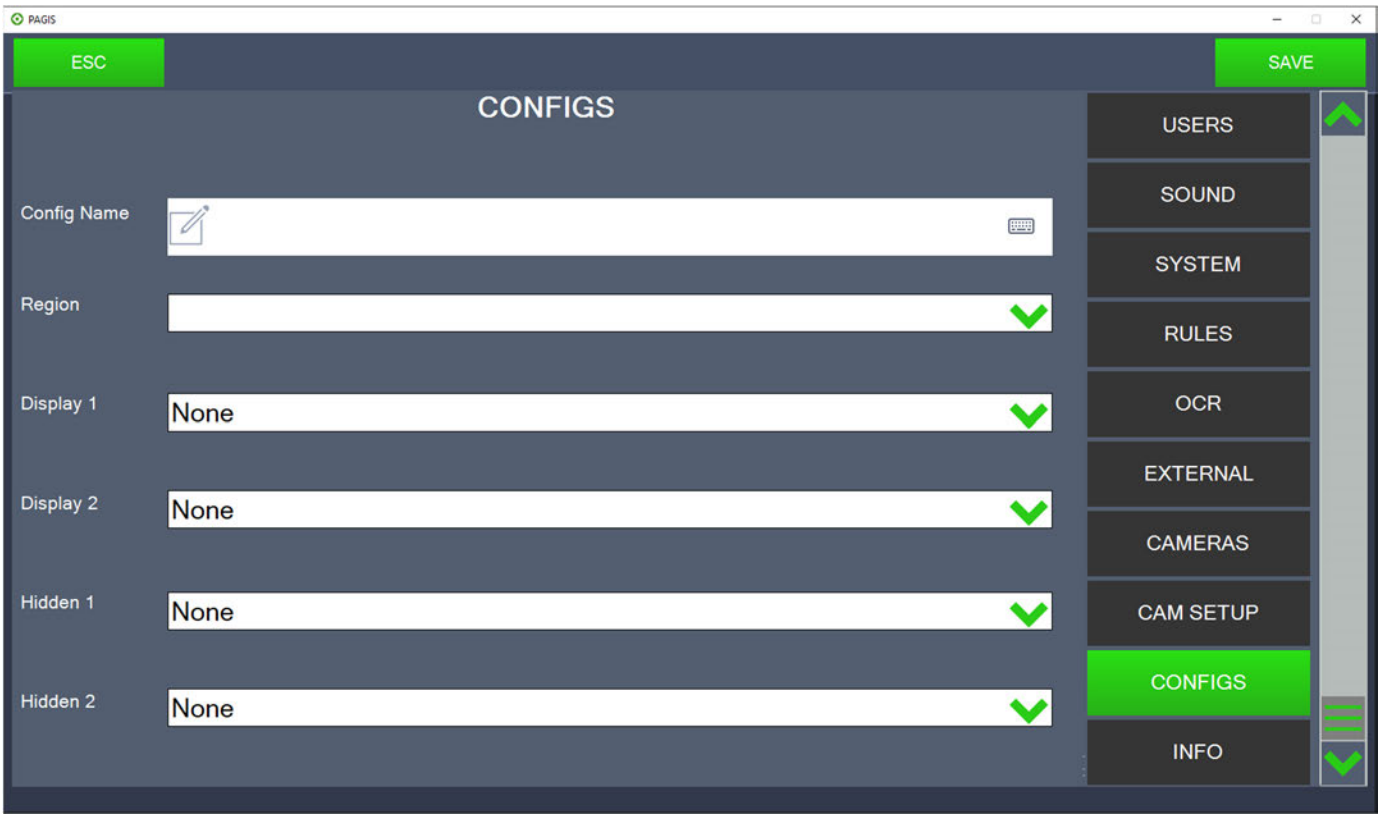


1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info

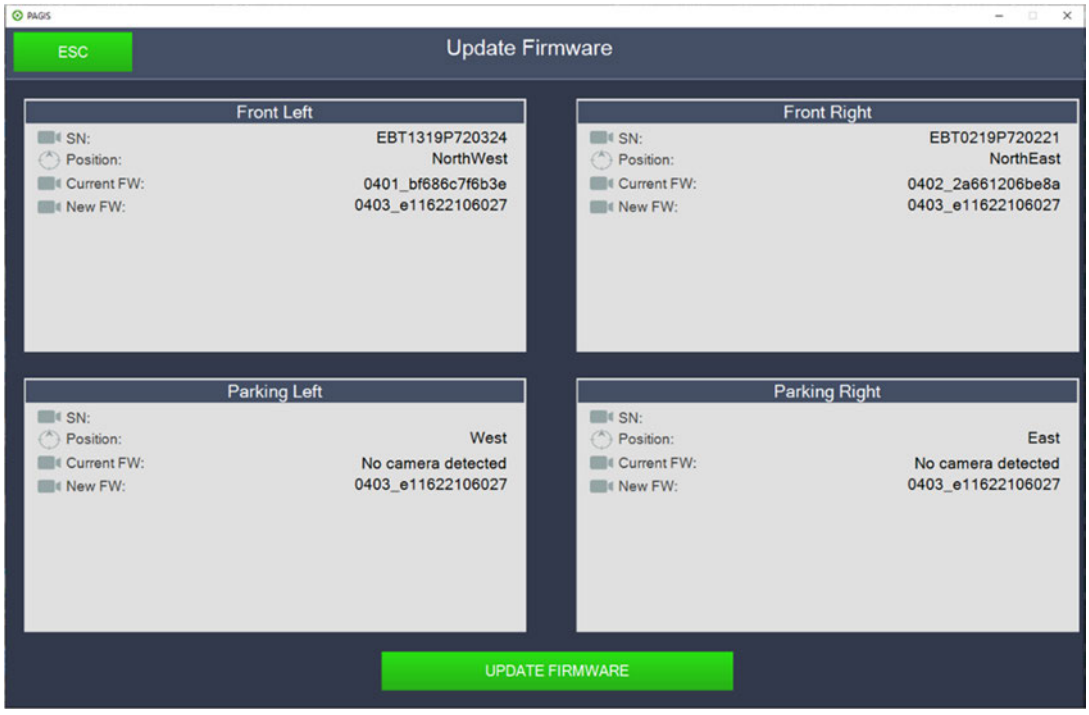
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The PIPS mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the PIPS mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the PIPS processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the 192.168.200.200 IP address, using alternative IP’s on MDC/Laptop will result in the software’s failure to communicate with the cameras when using VPRelay mode.

Alternative IP Network:

It is possible to configure the PIPS mobile processor to utilize a different IP network in conjunction with MDC/Laptop. Typical scenario would be when PIPS mobile processor and MDC/Laptop are connected through an onboard modem that has an Ethernet switch with available ports. Below are the general steps to changing IP network.

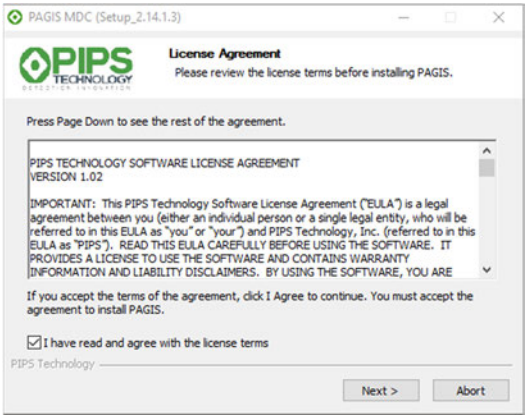
1. Follow the step above to connected to PIPS mobile processor.
2. Remote desktop to PIPS mobile processor and login using credentials provided in SX4 or SX4e manual.
3. In Windows “Services” find and stop the “PIPS VPRELAY” service.
4. Navigate to “C:\PIPSTechnology\VPRelay” and located file “anpr2.ini and open in notepad.
5. Alter “Address=192.168.200.102” to the IP your MDC/Laptop will assume after change to new network, save and close. The “PIPS VPRELAY” service will use this IP address to send camera data to PAGIS running on MDC/Laptop.
6. Alter PIPS mobile processors “Ethernet adapter 1” to new IP, refer to SX4 or SX4e manual for instruction on disabling the “WFManager” so change made to Ethernet are permanently saved.
7. Reboot PIPS mobile processor and enable “WFManager”.
8. Reassign IP on MDC/Laptop.
9. Start PAGIS on MDC/Laptop and confirm camera connectivity, if issues refer to FAQ’s in this manual for troubleshooting tips.

4.2.2 PAGIS Software Installation (MDC)

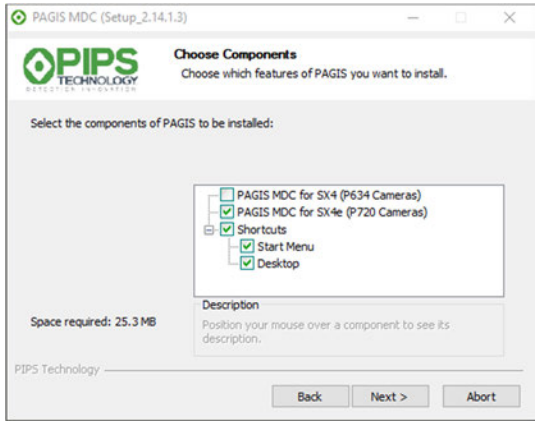
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select options so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor. If the 4 camera IO ports are vertically arranged RJ45’s then it’s a **SX4e(P720)**, if they are vertically arranged circular shaped “LEMO” connectors then it’s a **SX4(P634)**. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. Upgrading to PAGIS V2.14.x.x also requires that the PIPS mobile processor be updated to same version in order to take advantage of the Firmware updater feature.



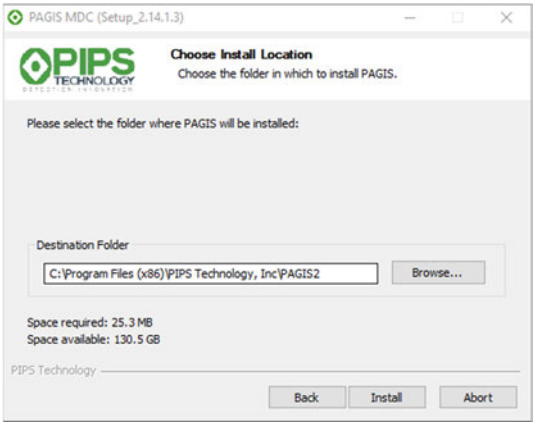
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



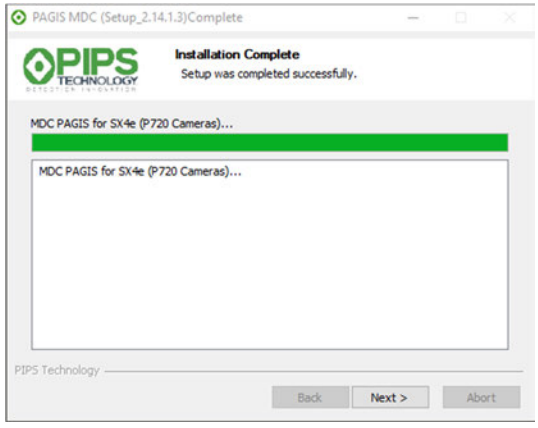
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

Note: See Appendix A for terminology definitions.

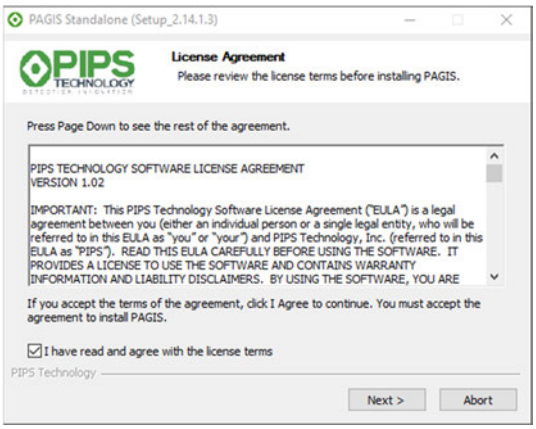
4.2.3 PAGIS Software Installation (Mobile Processor)

1. PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.

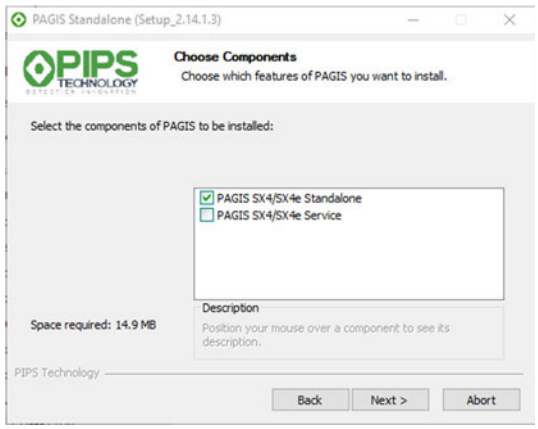
NOTE: If processor is in Service/VPRelay mode you MUST stop the “PIPS VPRELAY” service before running the updater.



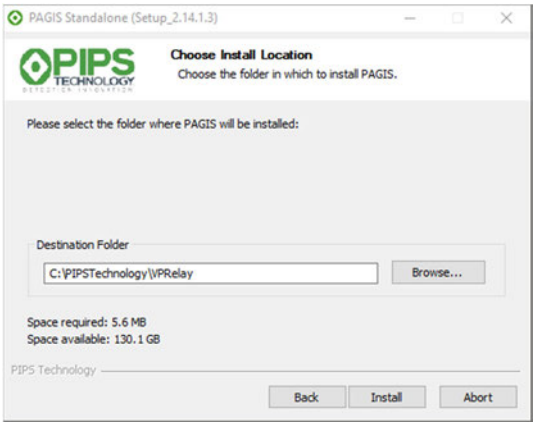
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



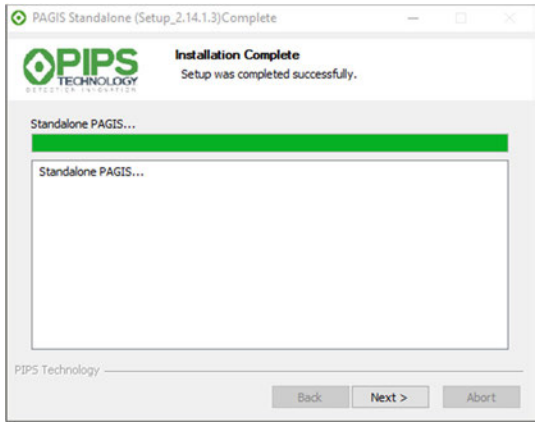
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

PAGIS/BOSS3 CONFIGURATION 977

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device. **NOTE**: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the “Hotlists” button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the “Deployment” field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be “built” or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating “HttpStatusCode” will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

980

ALPR/ANPR	“Automatic License Plate Recognition/Automatic Number Plate Recognition”.
BOSS	“Back Office System Software”. This is the ALPR server.
GPS	“Global Positioning System”.
GUI	“Graphical User Interface”.
Hotlist	A database or list that contains vehicle license plates of interest (“alert list”).
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	“Mobile Data Computer”. This is the tablet or laptop in the vehicle.
OCR	“Optical Character Recognition” (also referred to as a “cardet”).
OS	“Operating System”.
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or “VPRelay” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface. Same a “Service”
SX	SX is a short notation referencing PIPS’s mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A “User Interface” is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	“Vehicle License Plate”.
VPN	“Virtually Protected Network”.
VPRelay	Operation mode of the PAGIS software. VPRelay or “Service” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
  - If no value is defined, the field is placed as general information.
  - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
  - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
  - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Driver’s License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

To deploy a locally created hotlist to PAGIS without BOSS.

1. Create a folder called “beginshift” (Without Quotes) on the root drive of whatever drive media your using that PAGIS has access to, remember only on root drive, no subdirectory’s. Example C:\beginshift.
2. Place the .CSV & .INI in the newly created beginshift folder.
3. Log into PAGIS and configure Sync to access the drive where your file/files are located. When setting disk drive letter in PAGIS no need to indicate folder path as PAGIS assumes by default that “beginshift” exist on the root drive your selecting, refer to section 3.1 in this manual.
4. Go back to main screen and do beginshift.

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device

5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are

no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section “Cameras aren’t showing up in PAGIS anymore.”
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it’s plugged into the Left cam’s port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE’RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE’RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select “System” on the left pane
4. Confirm/Set the button at top to “Default”
5. Remove any value(s) stored in the GPS Connection String field. Leave ‘5’ in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn’t work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or “VPRelay Mode”. The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously

A: Settings > Update and Security > Windows Update > “Update History” link – if there, see the steps in the FAQ 987

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN’T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select “DWORD (32-bit)”
5. Name the new value “fMinimizeConnections”
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select “DWORD (32-bit)”
4. Name the new value “fMinimizeConnections”
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value “IgnoreNonRoutableEthernet”
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

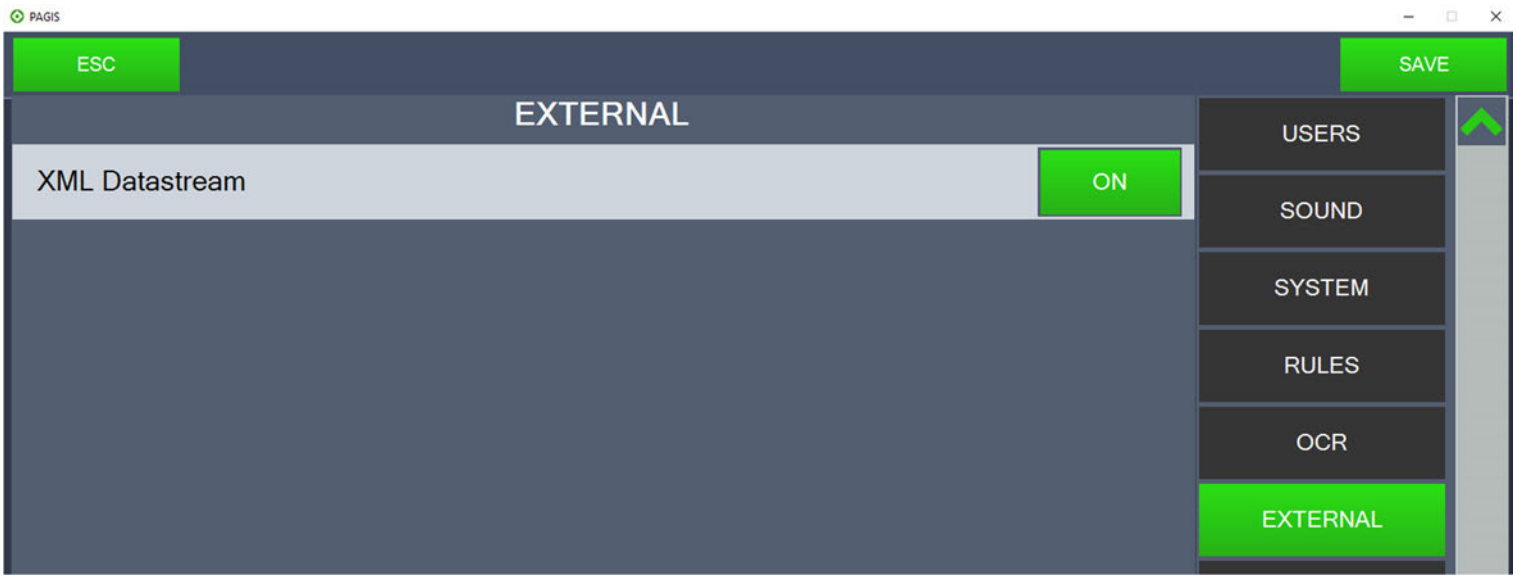
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD..................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS Administrator's Manual

Version 2.14

Updated 4/10/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.2.1 Getting Started in PAGIS 8

2.3 The PAGIS Navigation Buttons 9

2.3.1 Camera Control Buttons 9

2.3.2 GPS Indicators 10

2.3.3 Camera Firmware Update (Restricted Users) 10

2.3.4 Day/Night Mode 10

2.4 Begin Shift 11

2.4.1 Sync via USB Thumb drive (or Local Source) 11

2.4.2 Sync via Wireless Network 11

2.4.3 PAGIS Auto-Sync Settings 11

2.4.4 Begin Shift – Additional Information 11

2.5 End Shift 11

2.5.1 Sync to BOSS 11

2.6 Cam Mode Button 12

2.6.1 Camera Modes 12

2.7 Taking a Picture 12

2.8 Search Entry Screen 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits 13

2.8.2.1 Searching for a Match 14

2.8.3 Wild Card Symbols 14

2.8.4 Manually Adding a Plate to PAGIS 15

2.8.4.1 ADD VLP Query 15

2.8.4.2 ADD VRM Report Screen 15

2.9 The Review Screen 16

2.9.1 Summary Review Section 16

2.9.2 Review Navigation Buttons 16

2.9.3 Reads 17

2.9.3.1 Reads Result Screen Navigation Buttons 17

2.9.3.2 Interactive Buttons – Reads Screen 17

2.9.4 Hits 18

2.9.4.1 Hit Screen Attributes 18

2.9.4.2 Hit Screen Function Buttons 19

2.9.4.3 Interactive Buttons – Hits Screen 19

2.9.4.4 Set Disposition – Additional Detail 19

2.9.4.5 Add Intel – Additional Detail 20

2.9.5 Misreads 20

2.9.5.1 Marking a Record as a Misread: 21

2.9.6 Audits 22

2.9.7 Targets 22

2.9.7.1 The Targets Screen 23

2.9.7.2 Targets Screen Navigation Buttons 23

2.9.8 Databases 24

2.9.8.1 Databases Screen Functions 24

2.9.8.2 Databases Screen Navigation Buttons 24

2.9.8.3 Databases Edit- “Manual Reports” 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization Types 26

3.1.1.1 Synchronization to Disk (Local Storage) 27

3.1.1.2 Synchronization with BOSS 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 28

3.1.2 Global Sync Options 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

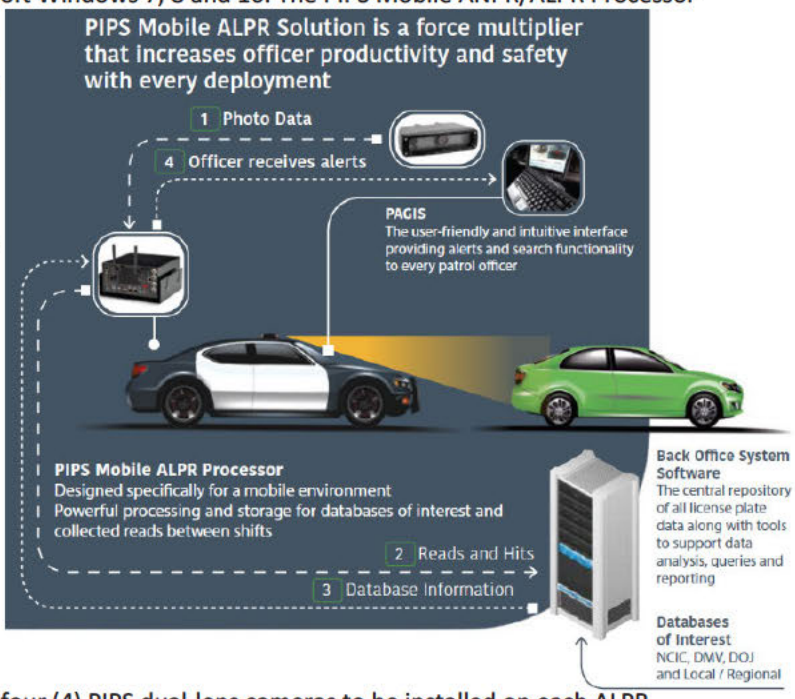
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

996

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

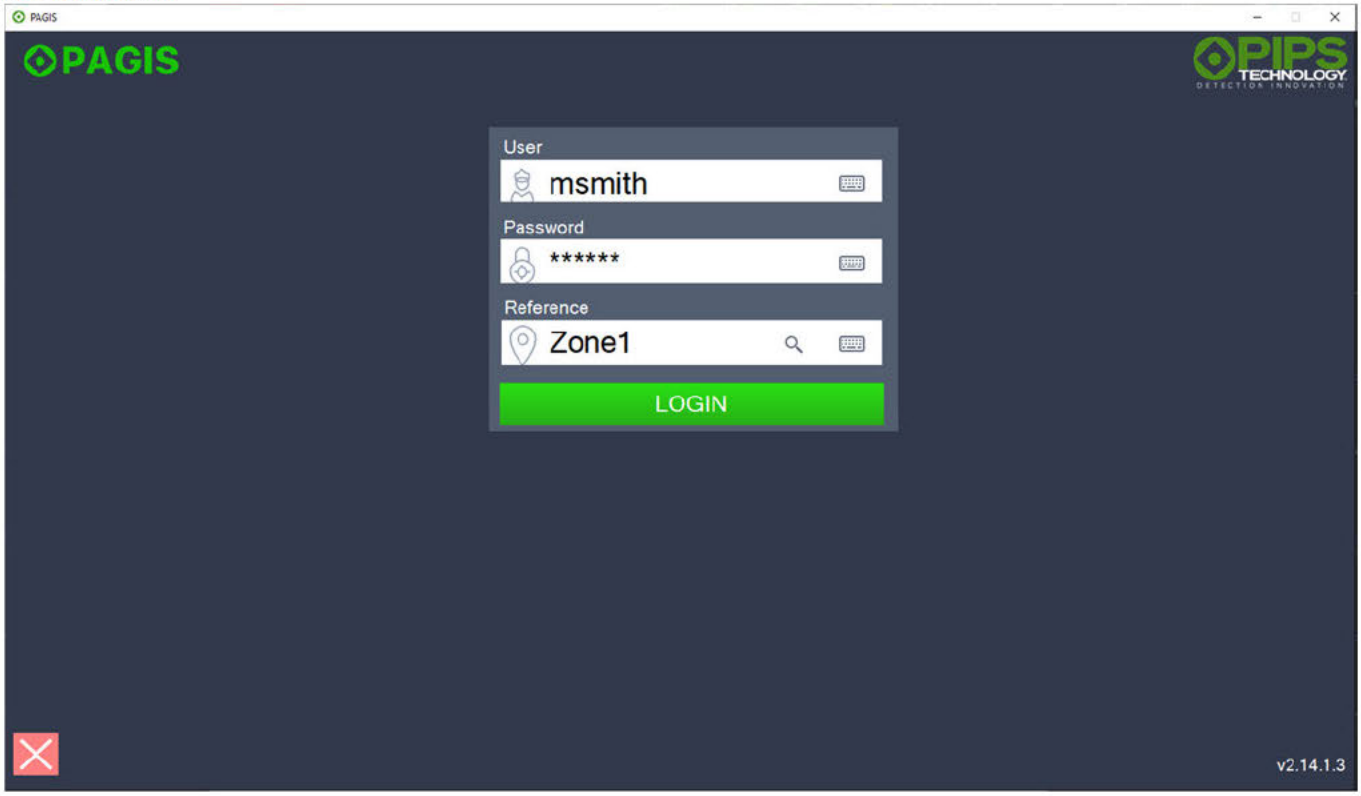
Section 5: Additional Information and Troubleshooting Tips

Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

998

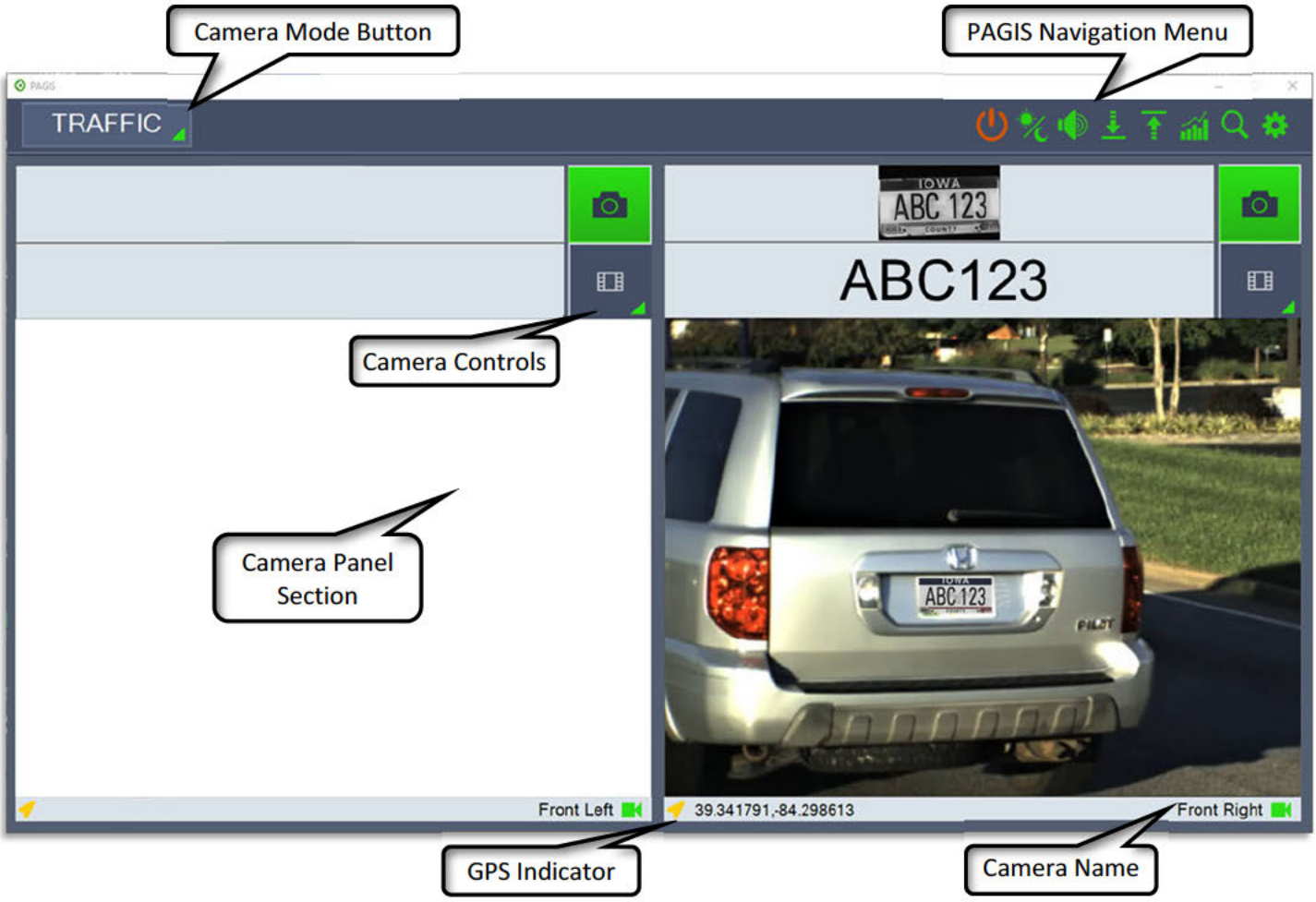
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

999

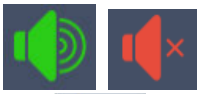
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

1000

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

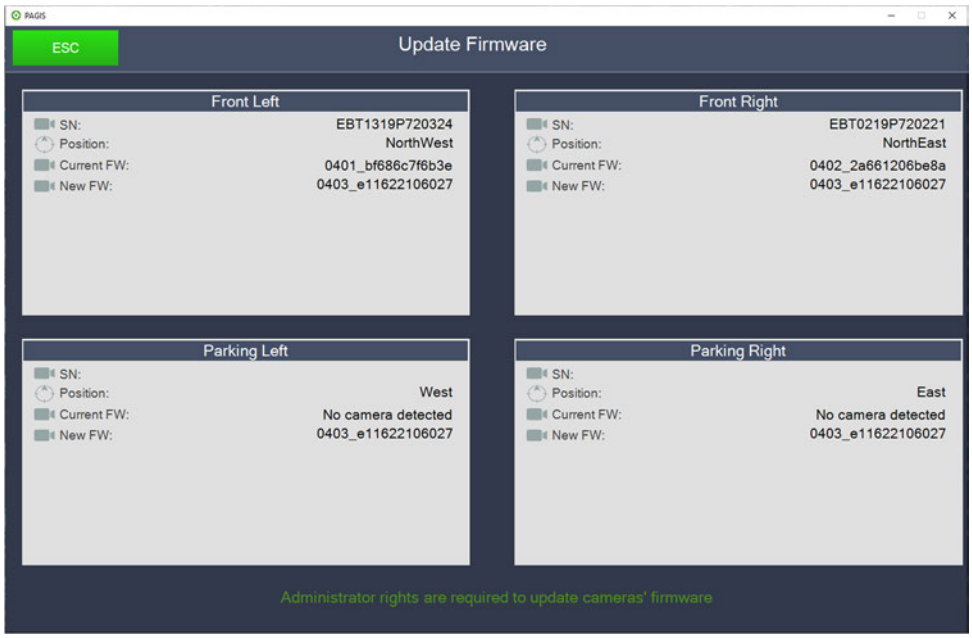
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

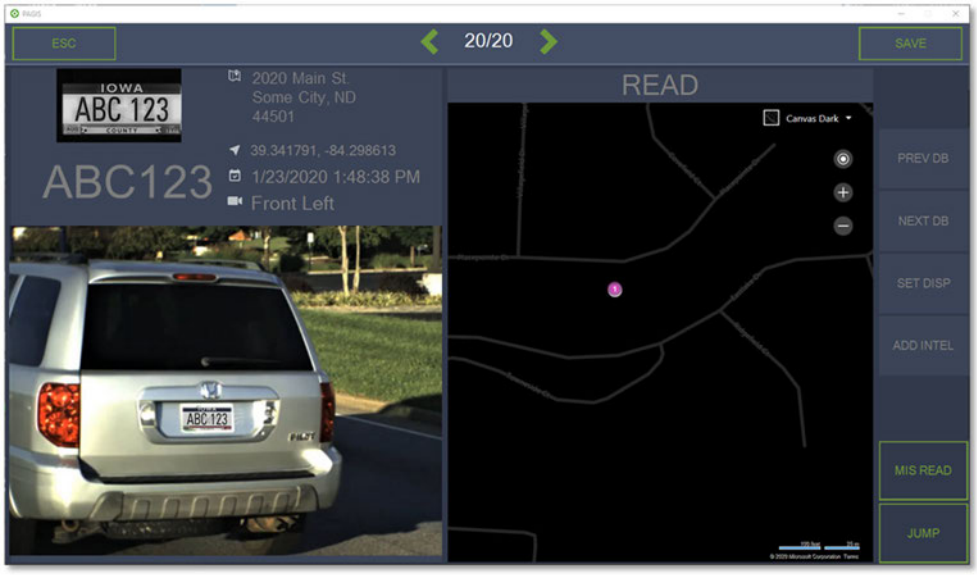


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

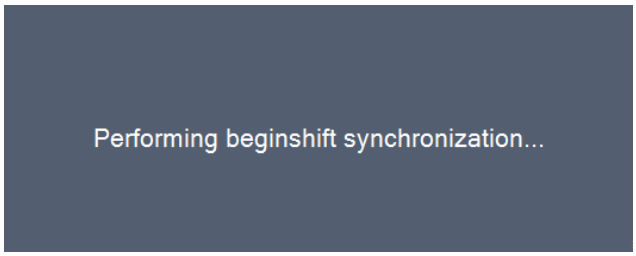
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

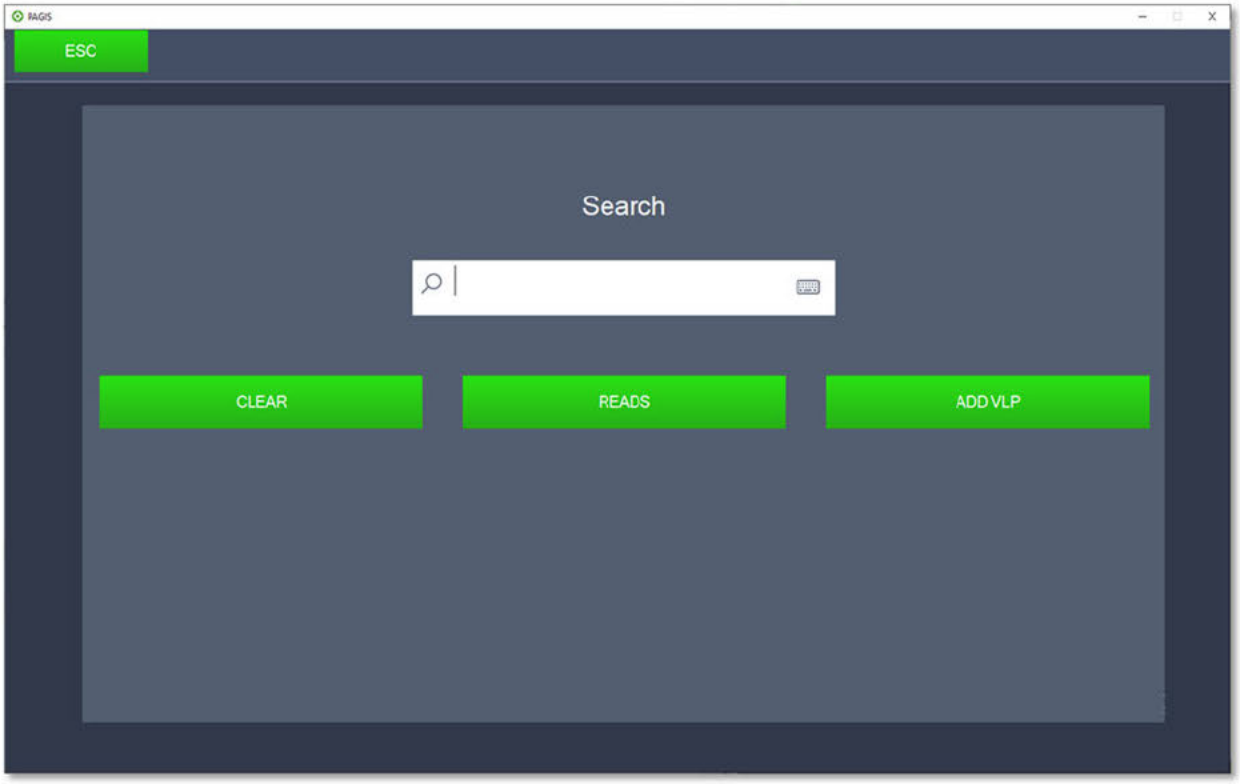
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

1004

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

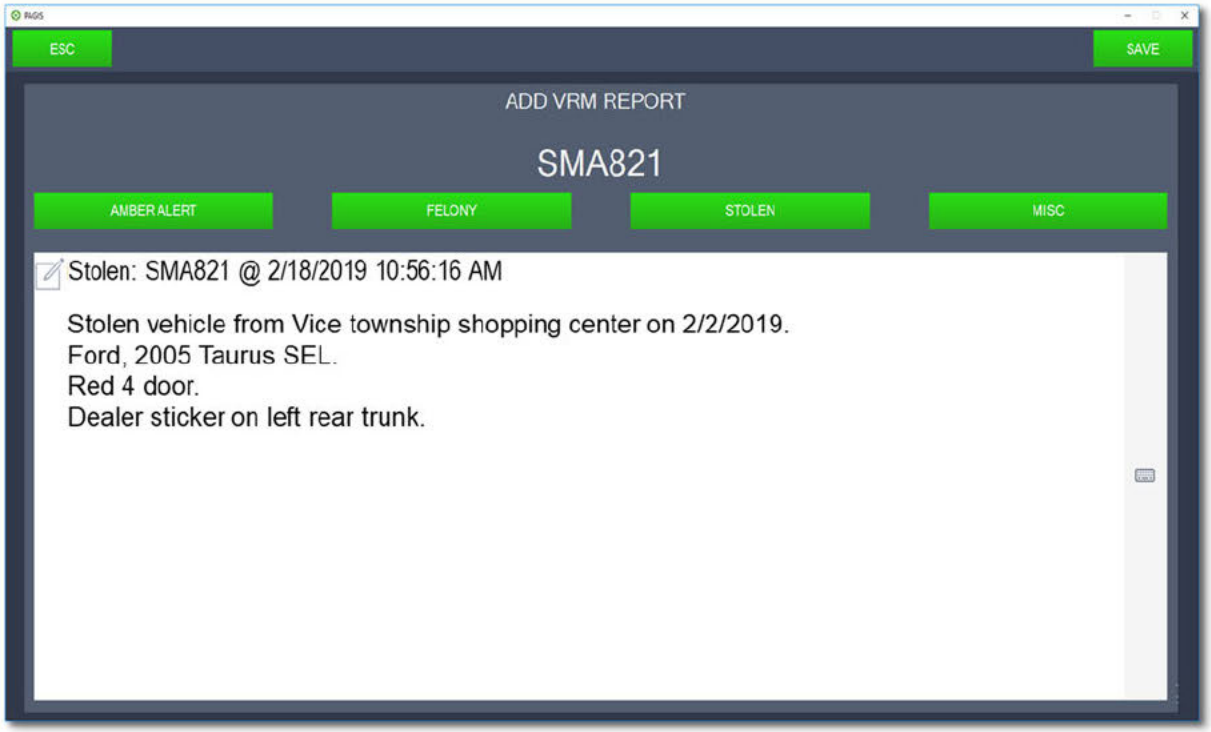
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

1006

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

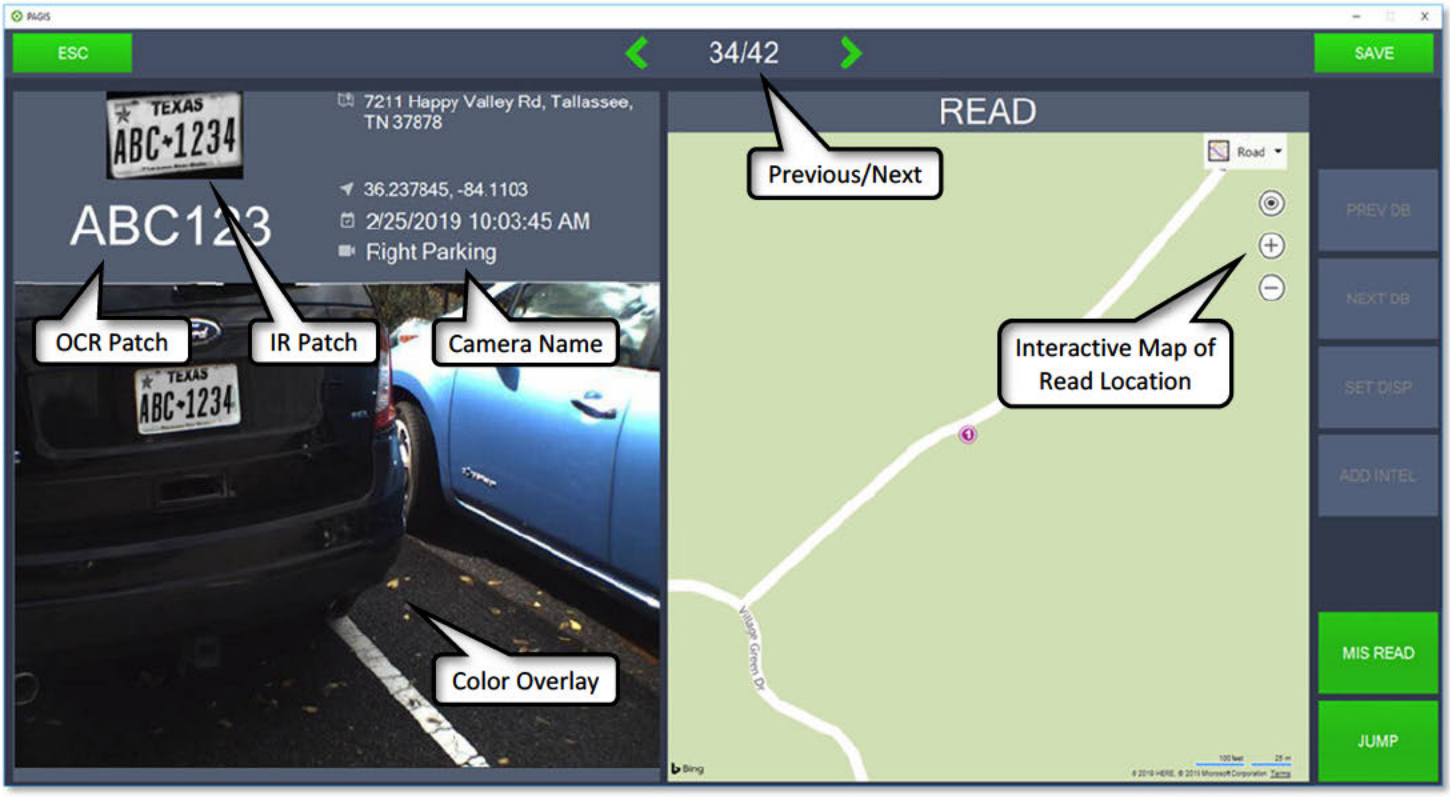
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

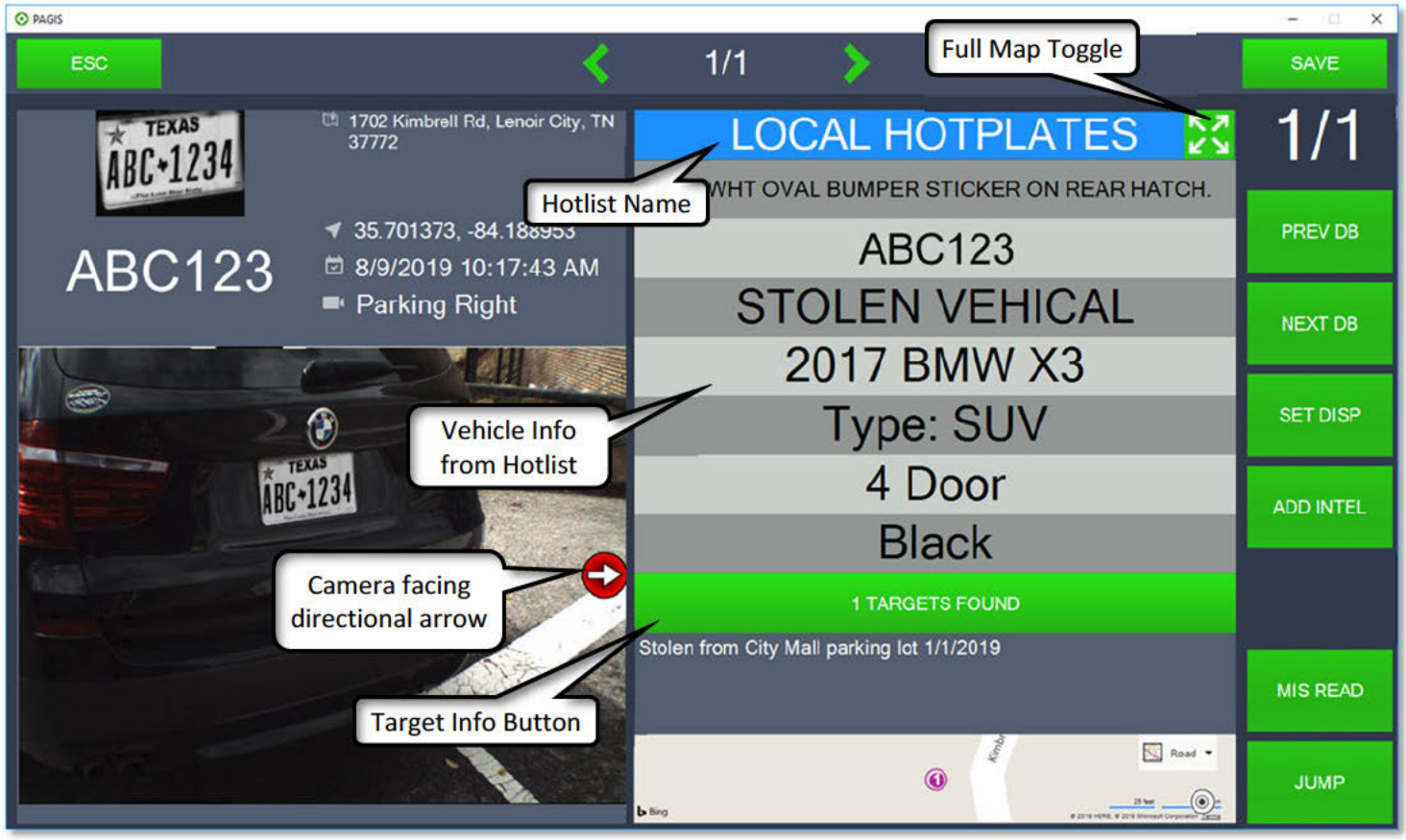
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail



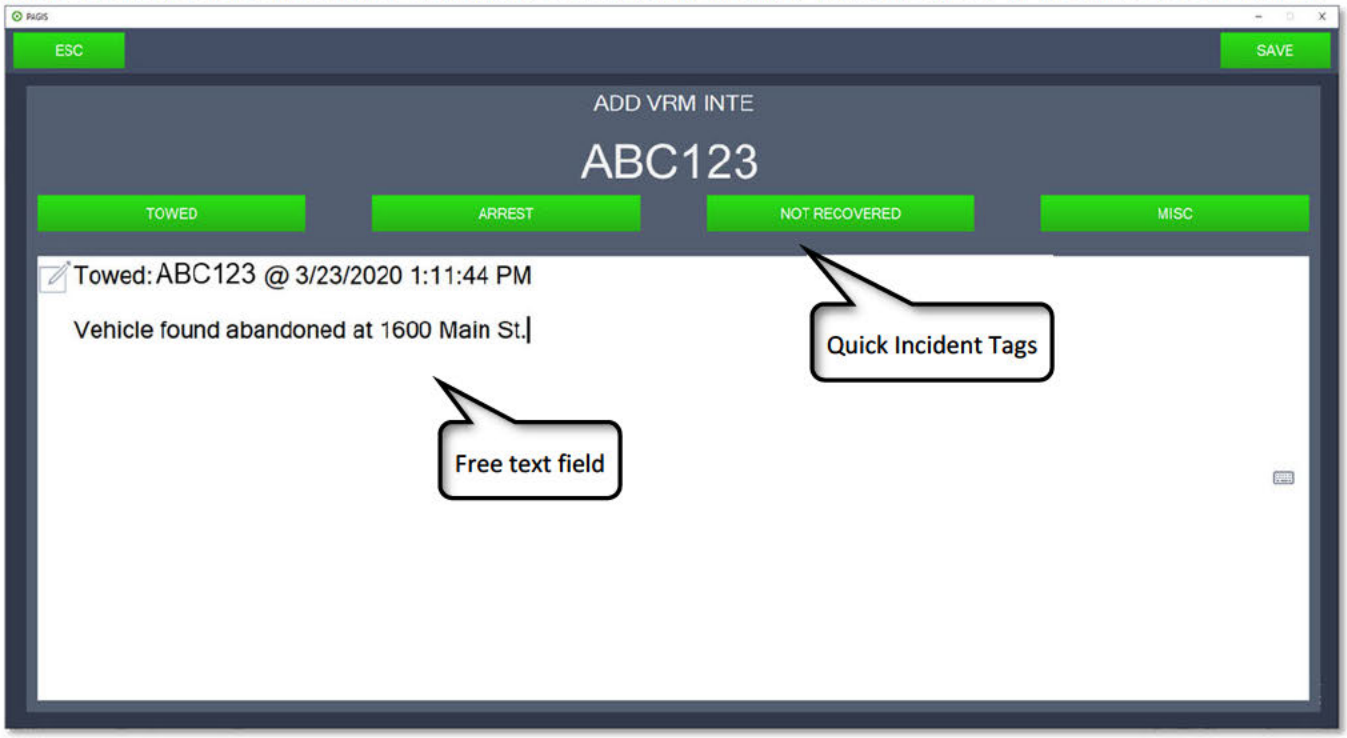
PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

1010

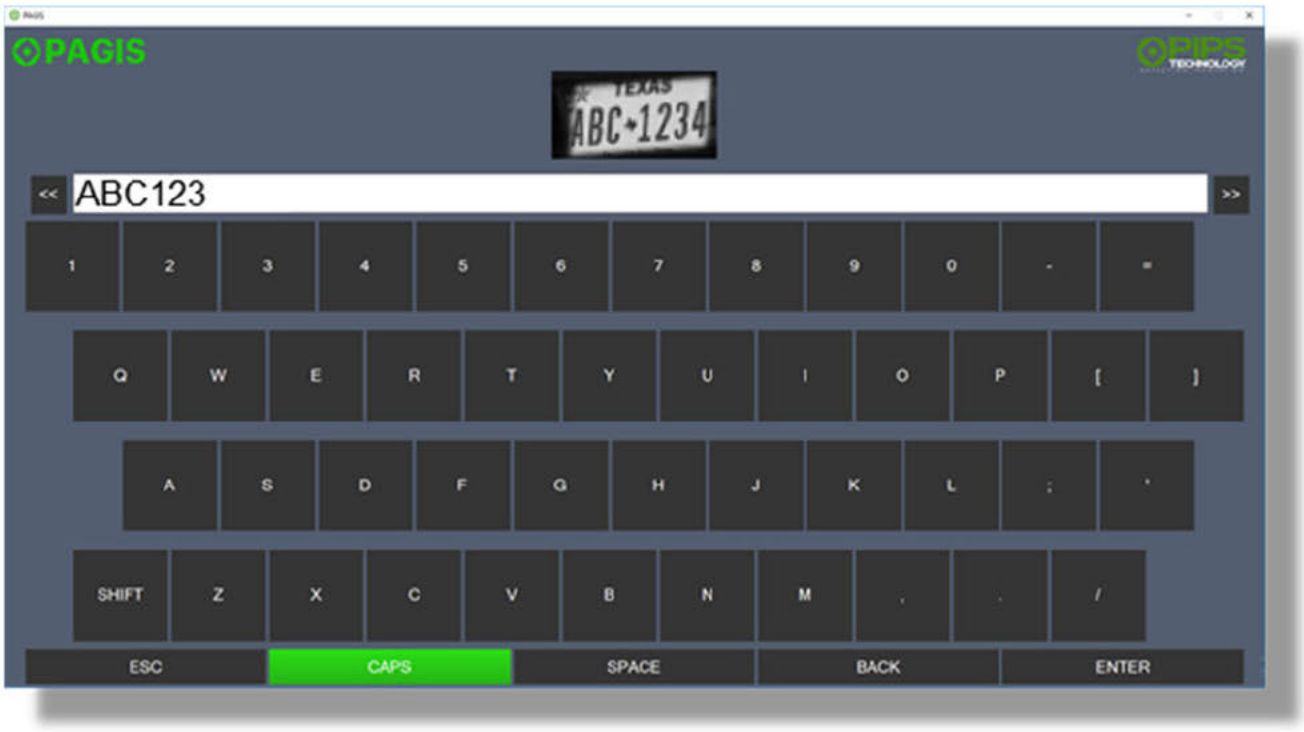
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

Updating the Read/Hit OCR Patch:

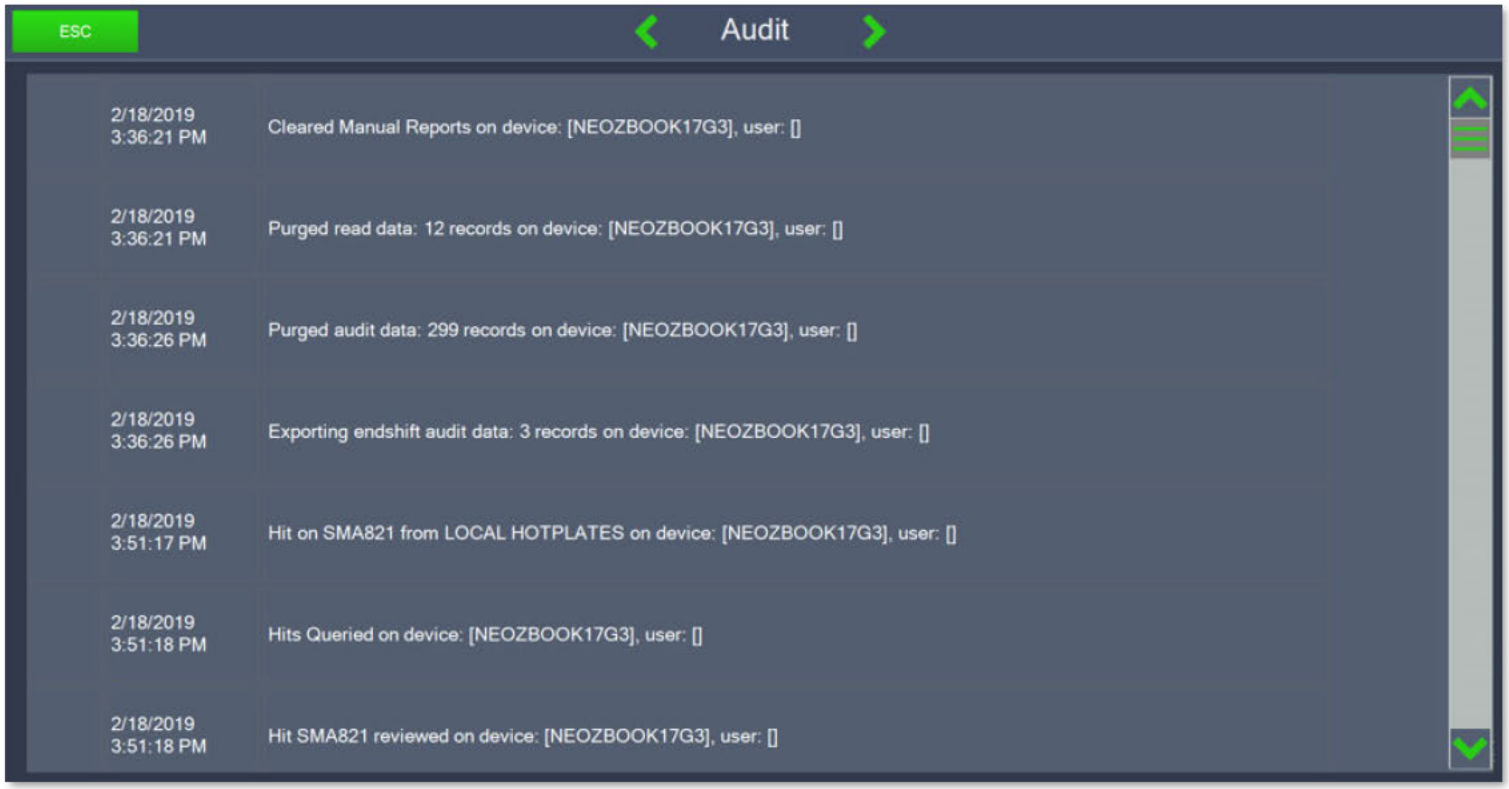
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

1012

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



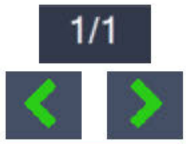
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

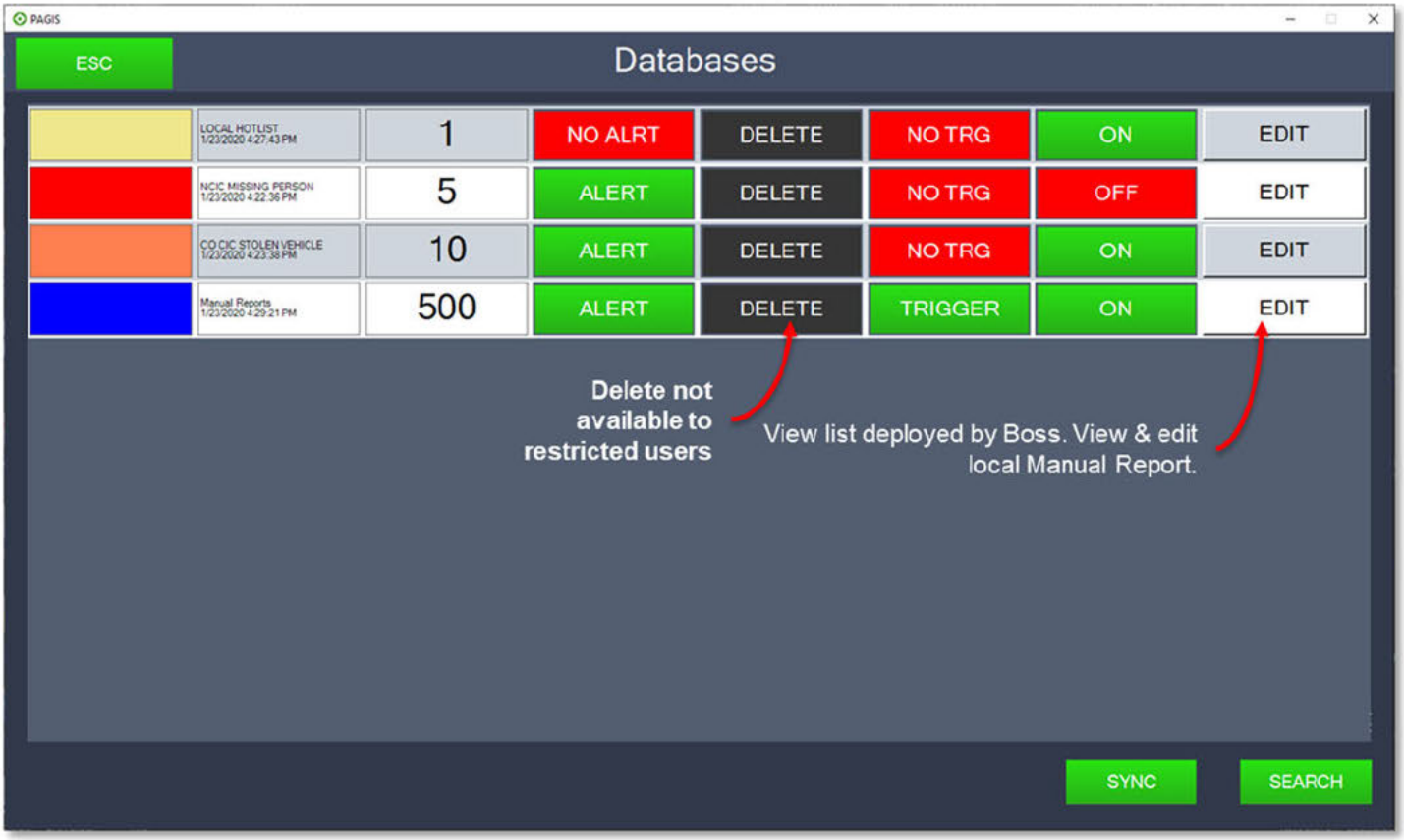


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

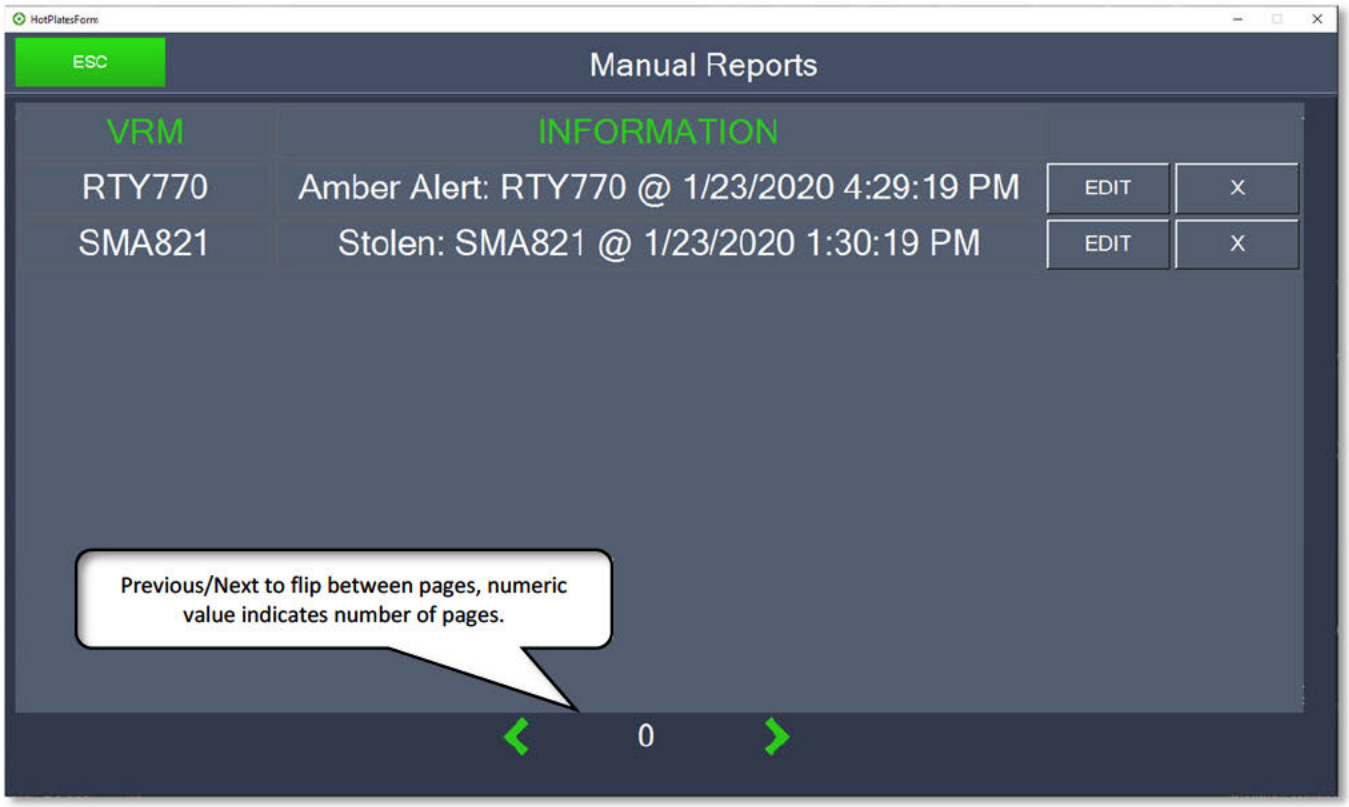
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



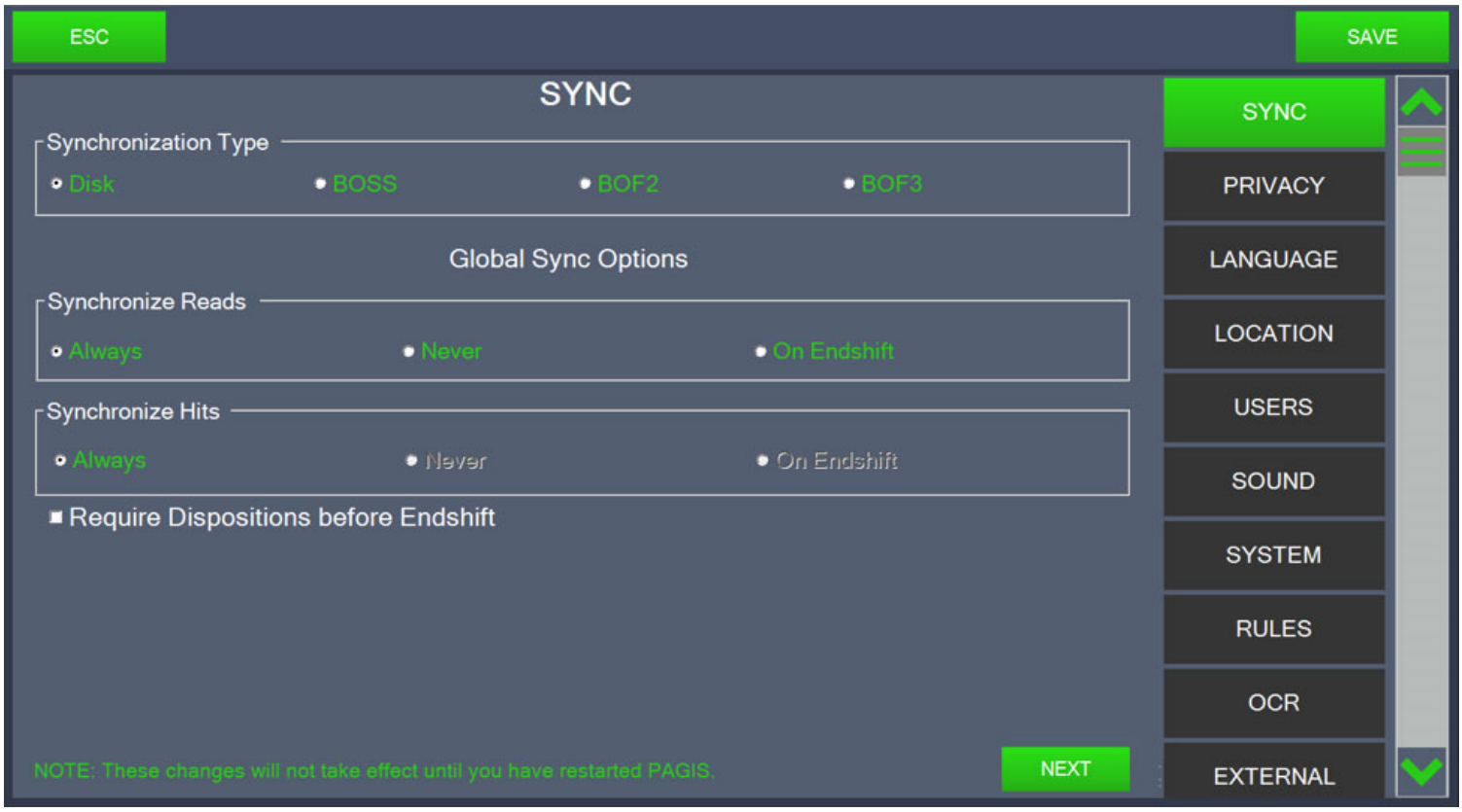
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

1017

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

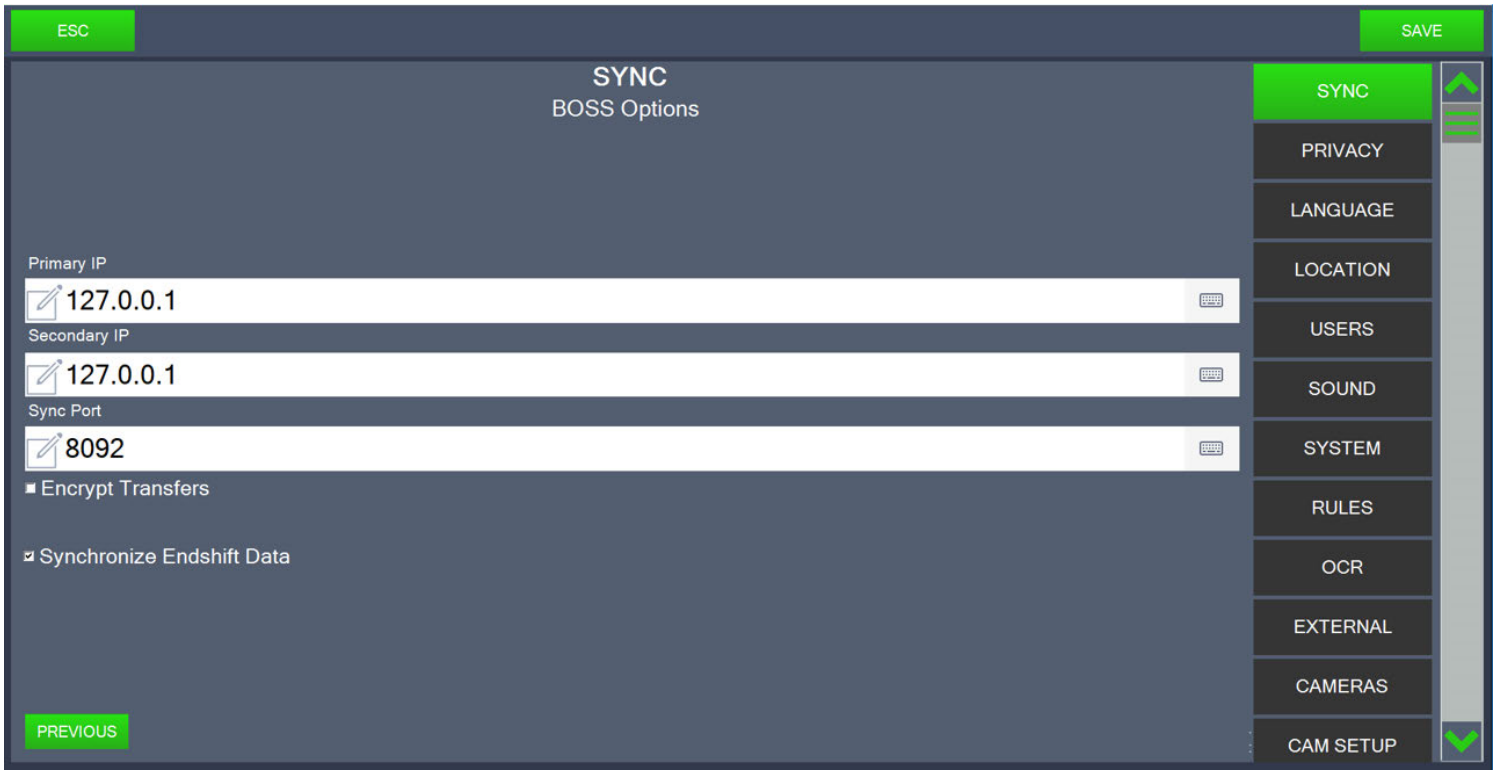


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

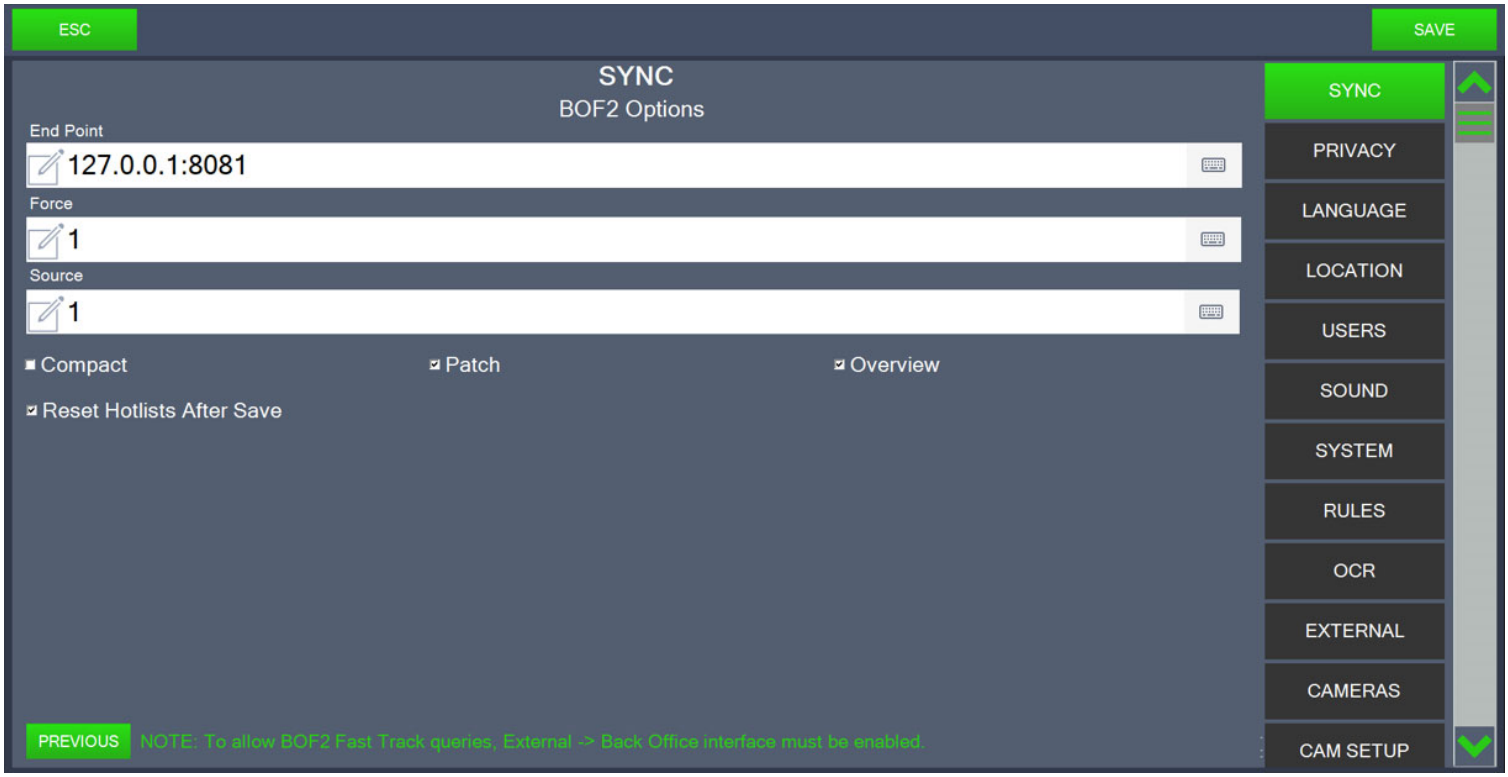
- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:
To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)
NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the PIPS BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.

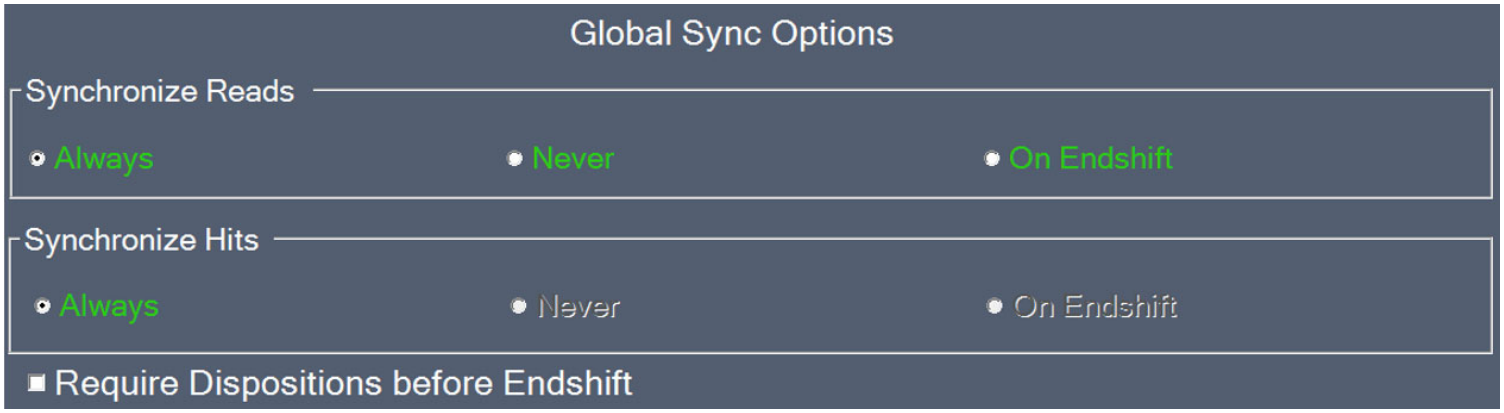


- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

1019

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



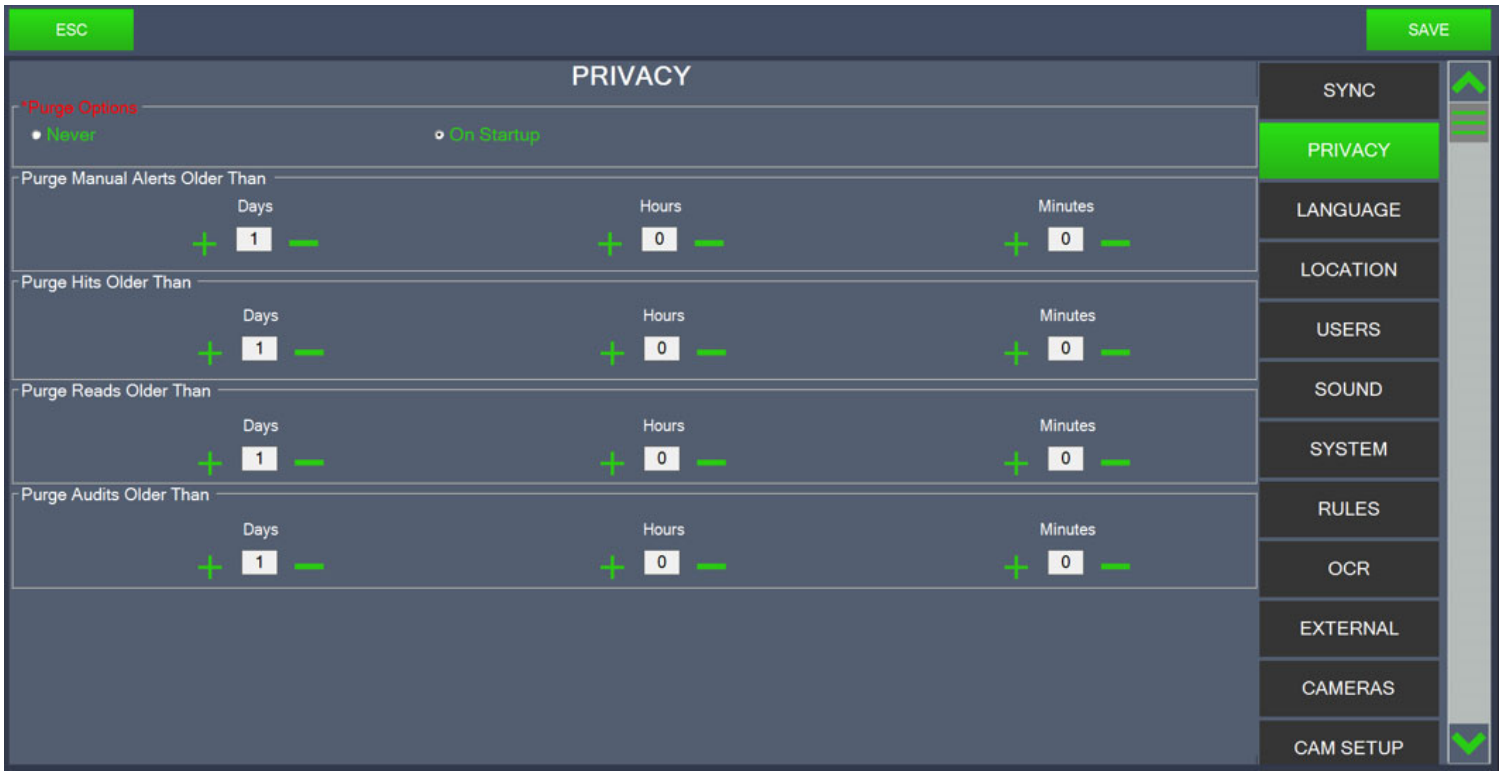
NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

1020

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

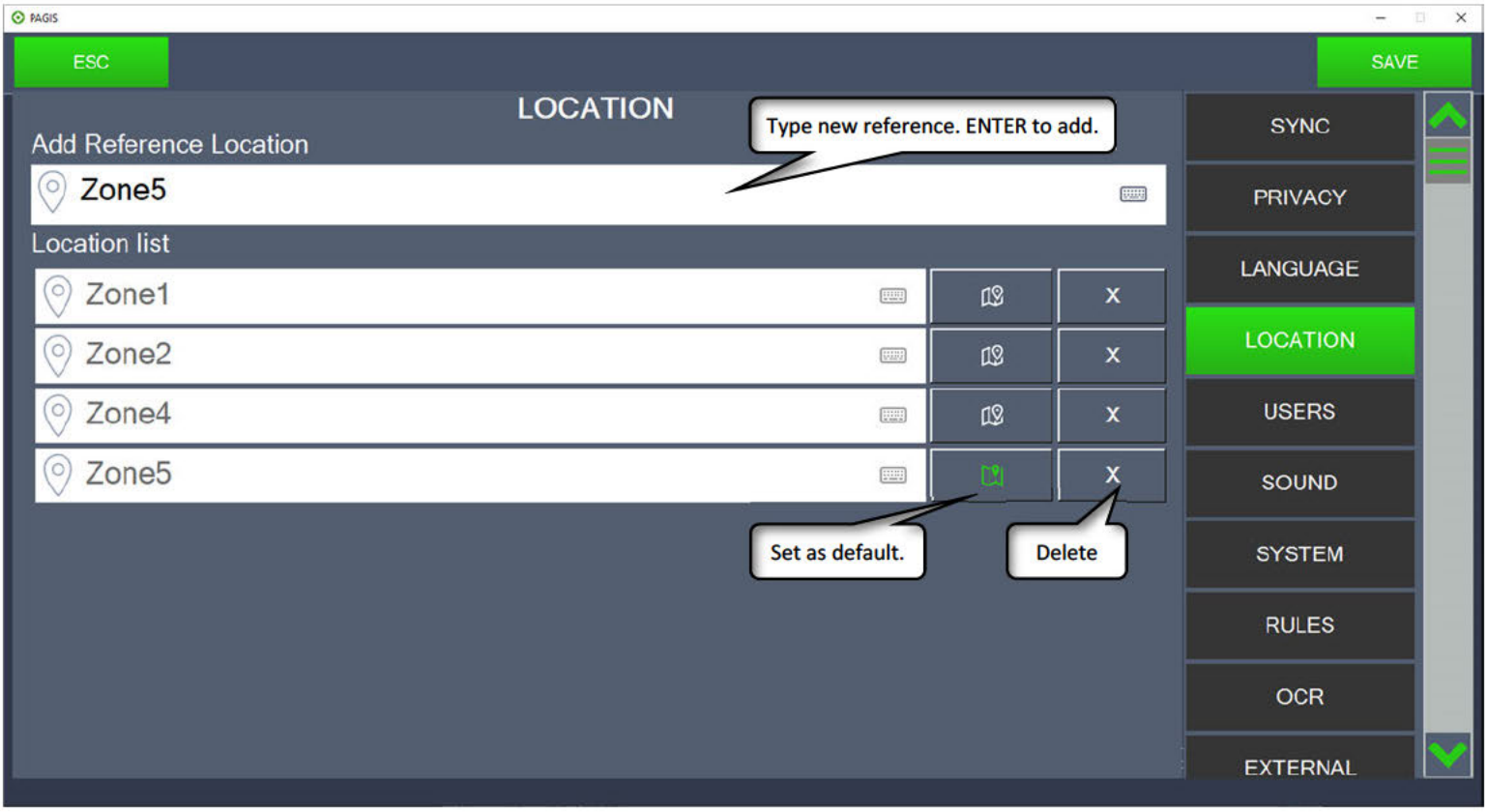
NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

3.3 Language

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

3.4 Location

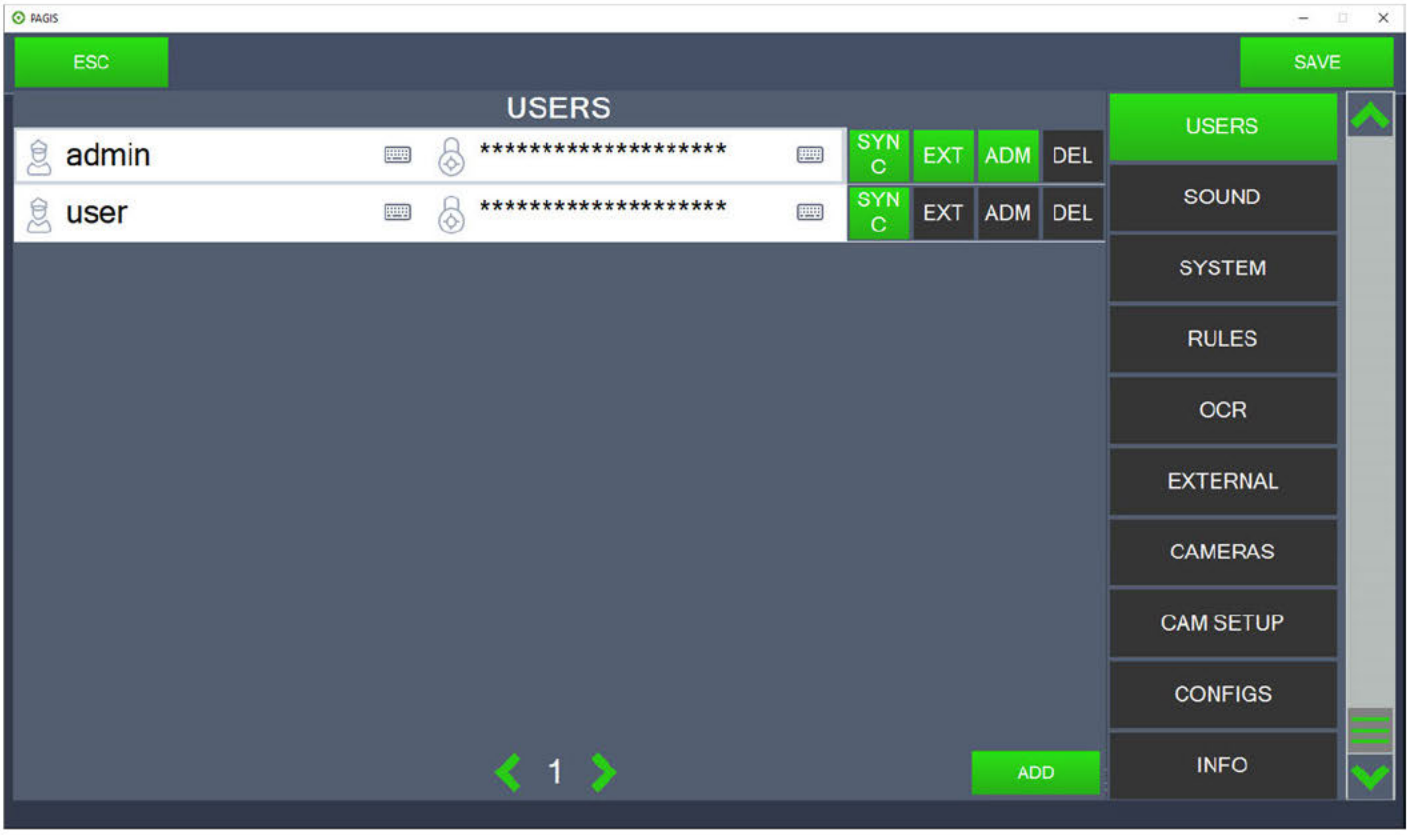
Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users

1022

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

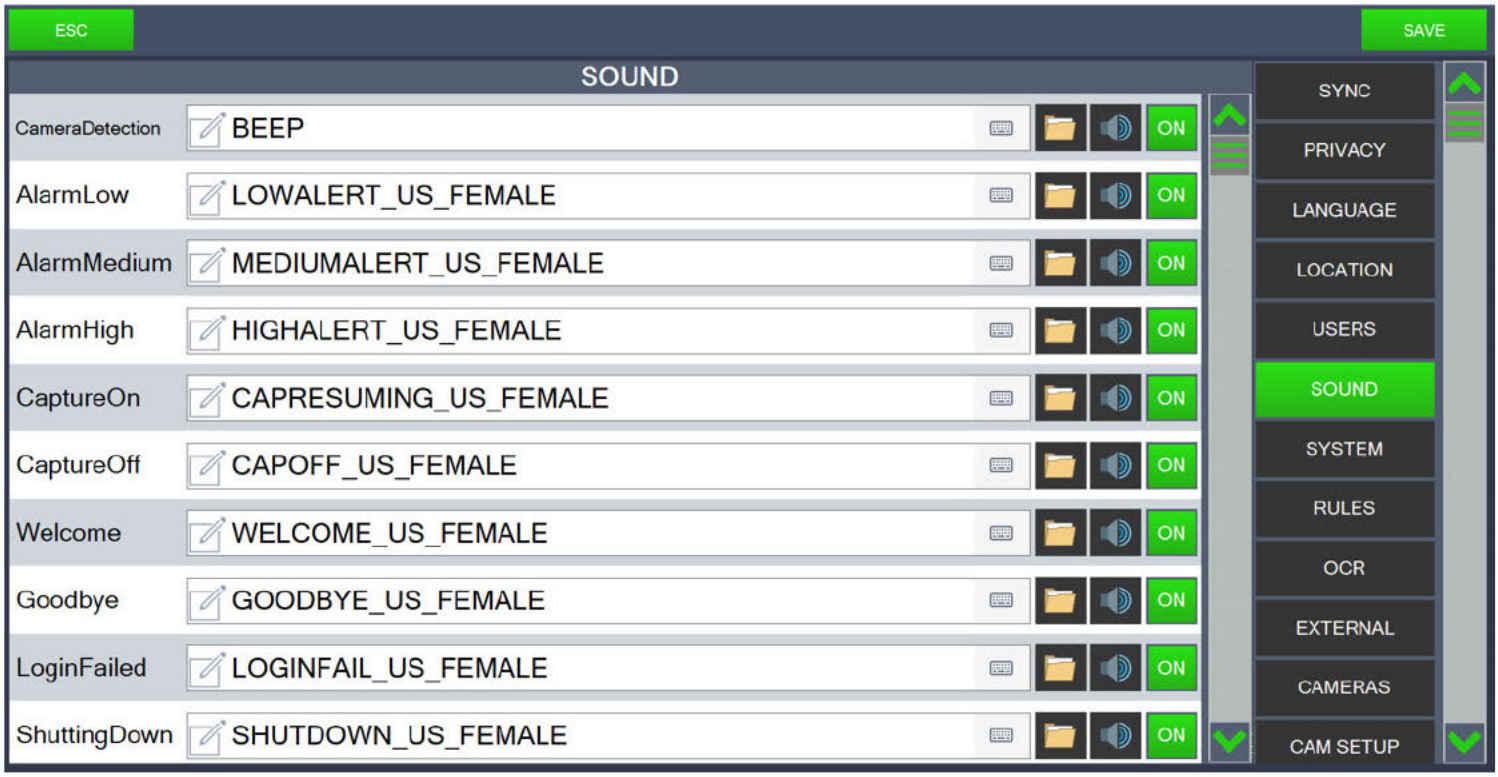
ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



Shows the status of that sound. Click to turn each sound Off.

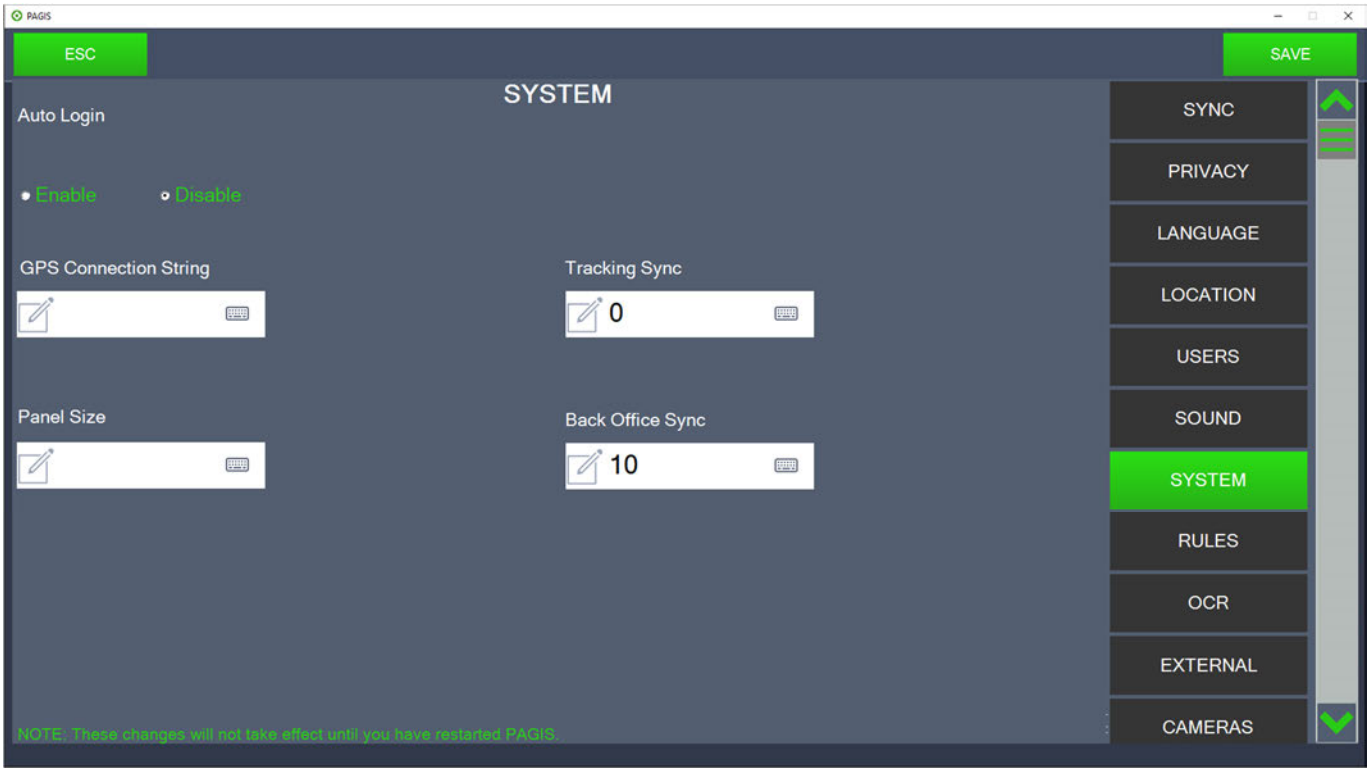


Shows the status of that sound. Click to turn each sound On.

3.7 System

1024

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).

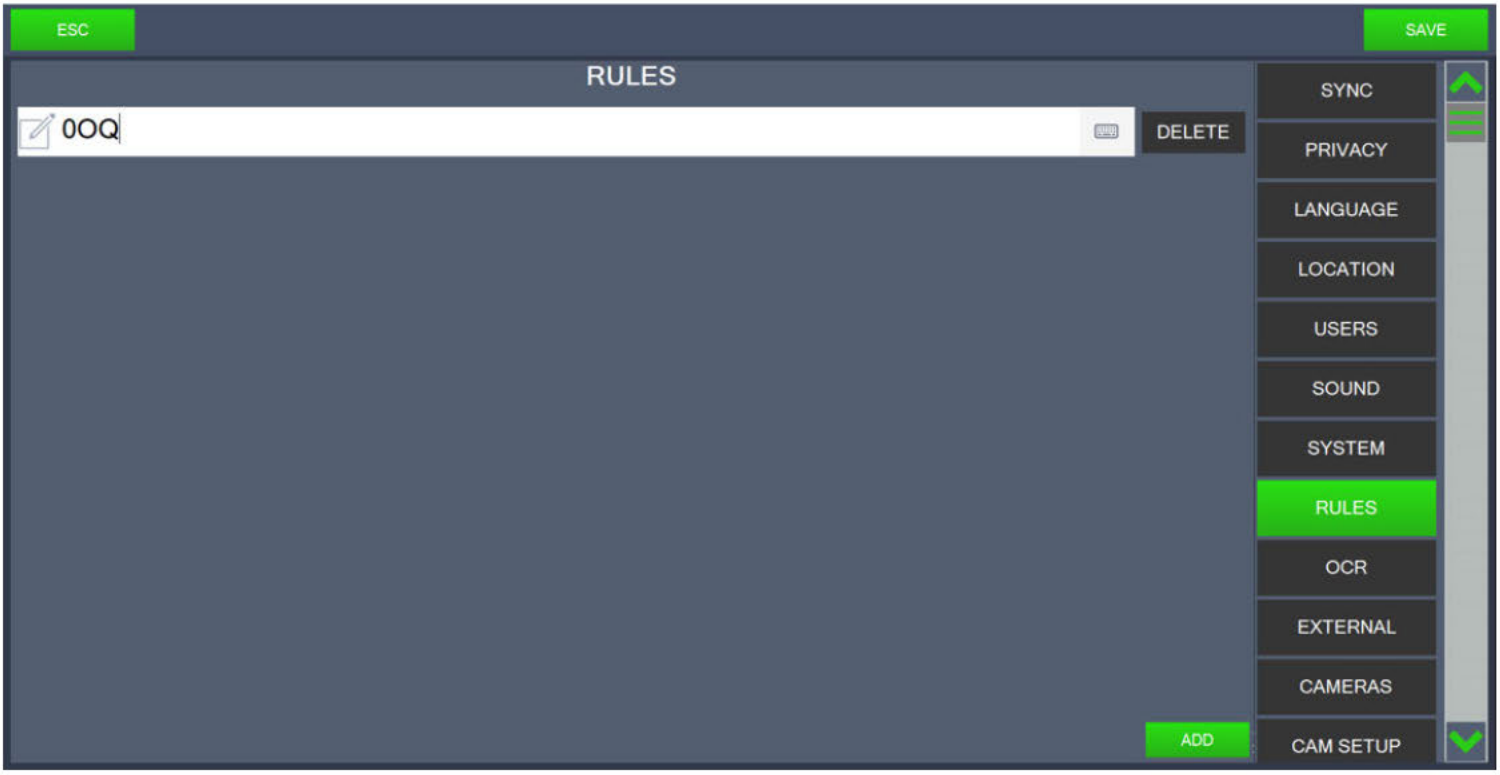


- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of PIPS Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

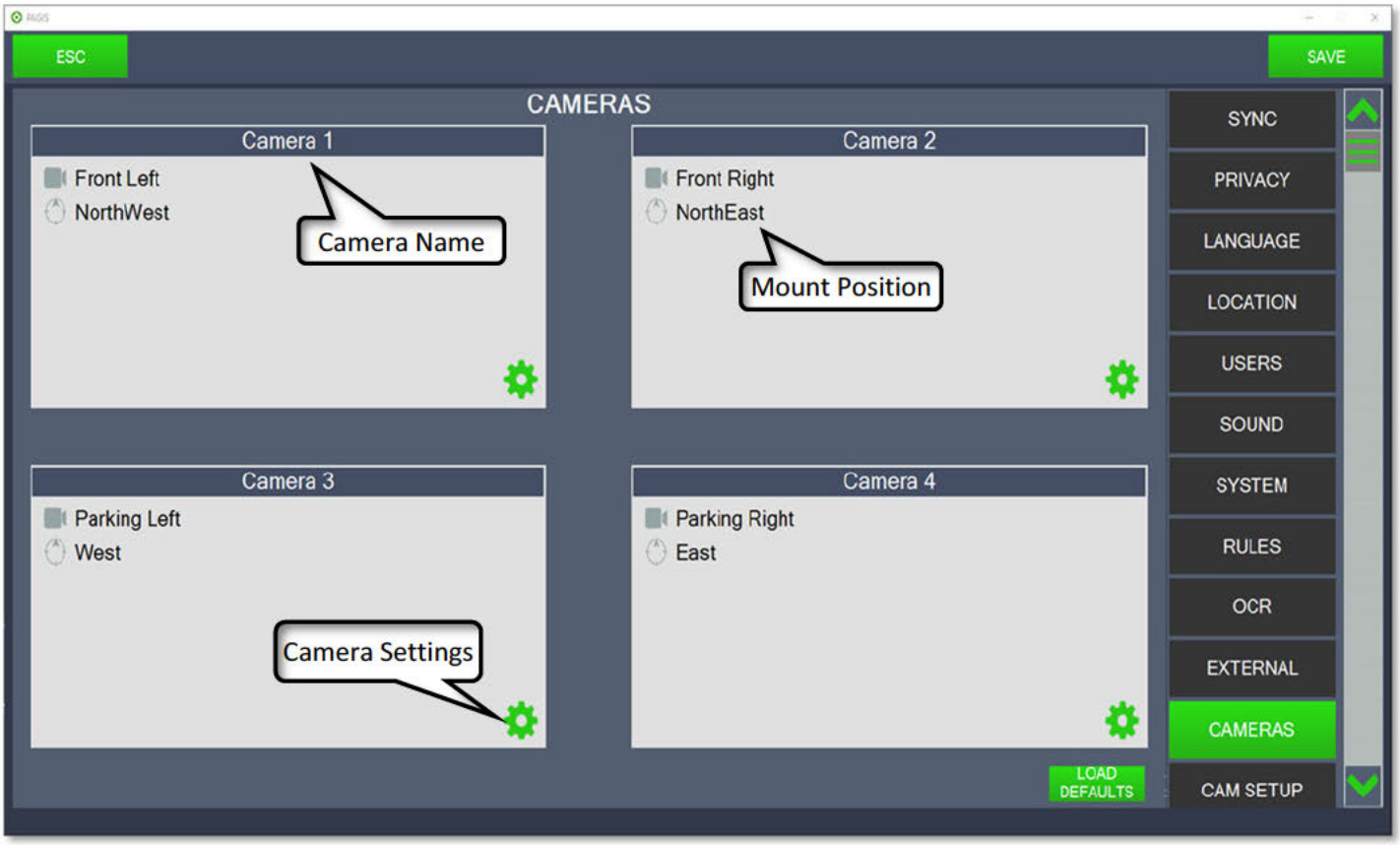
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

3.11 Cameras

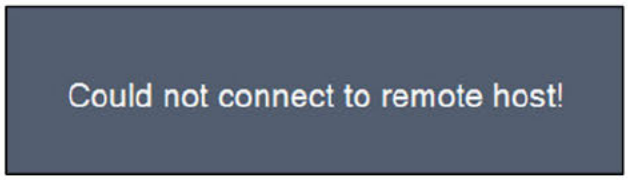
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

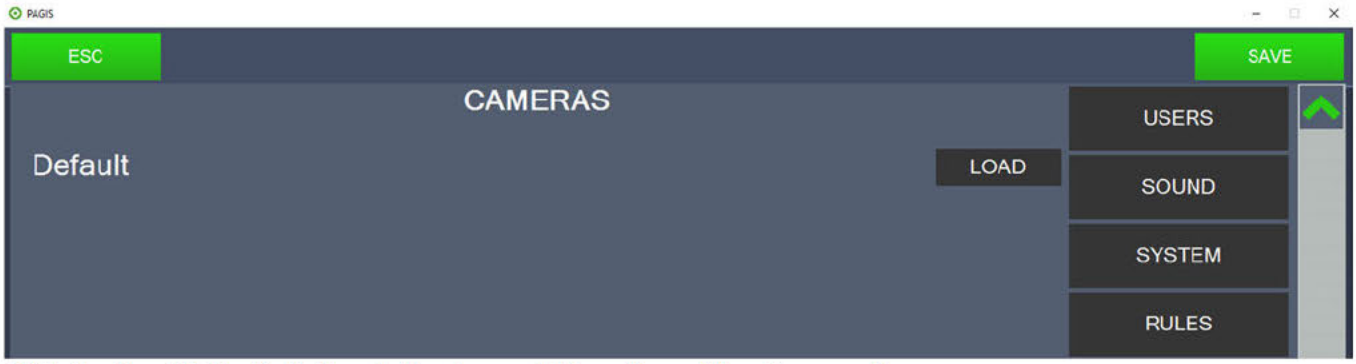
The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact PIPS Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button LOAD DEFAULTS. This manual will start with Load Defaults.

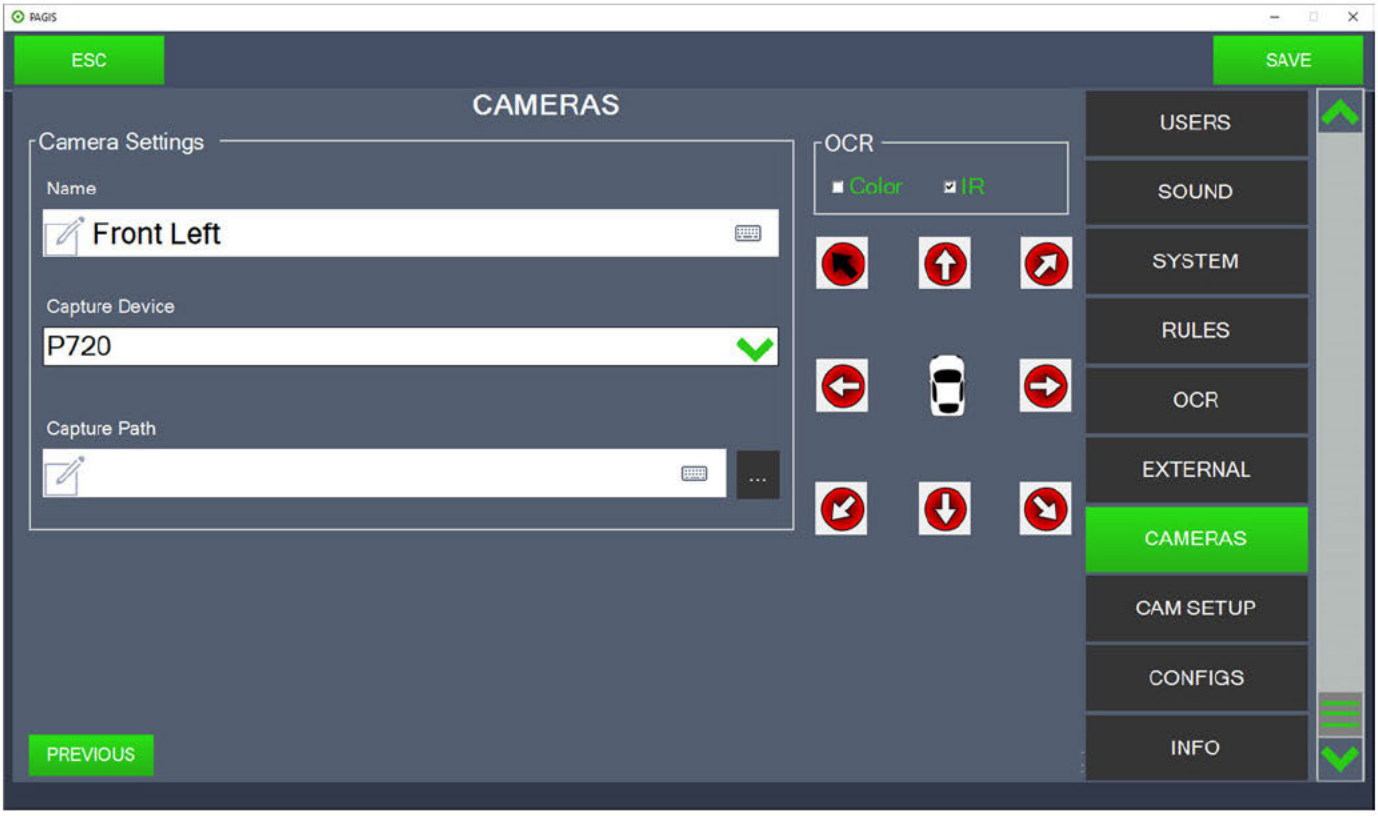
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button LOAD
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

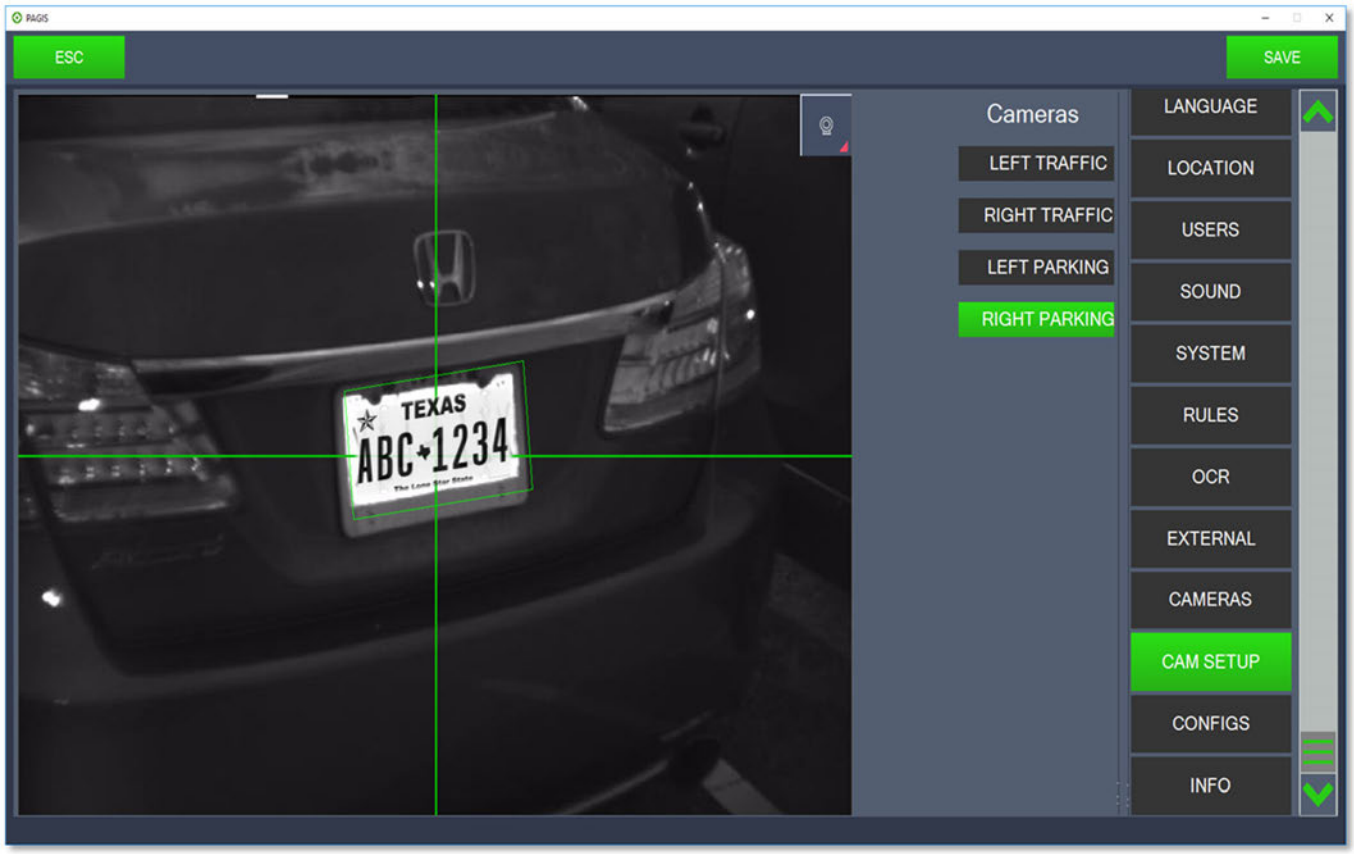
This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.



1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

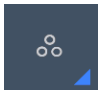
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.

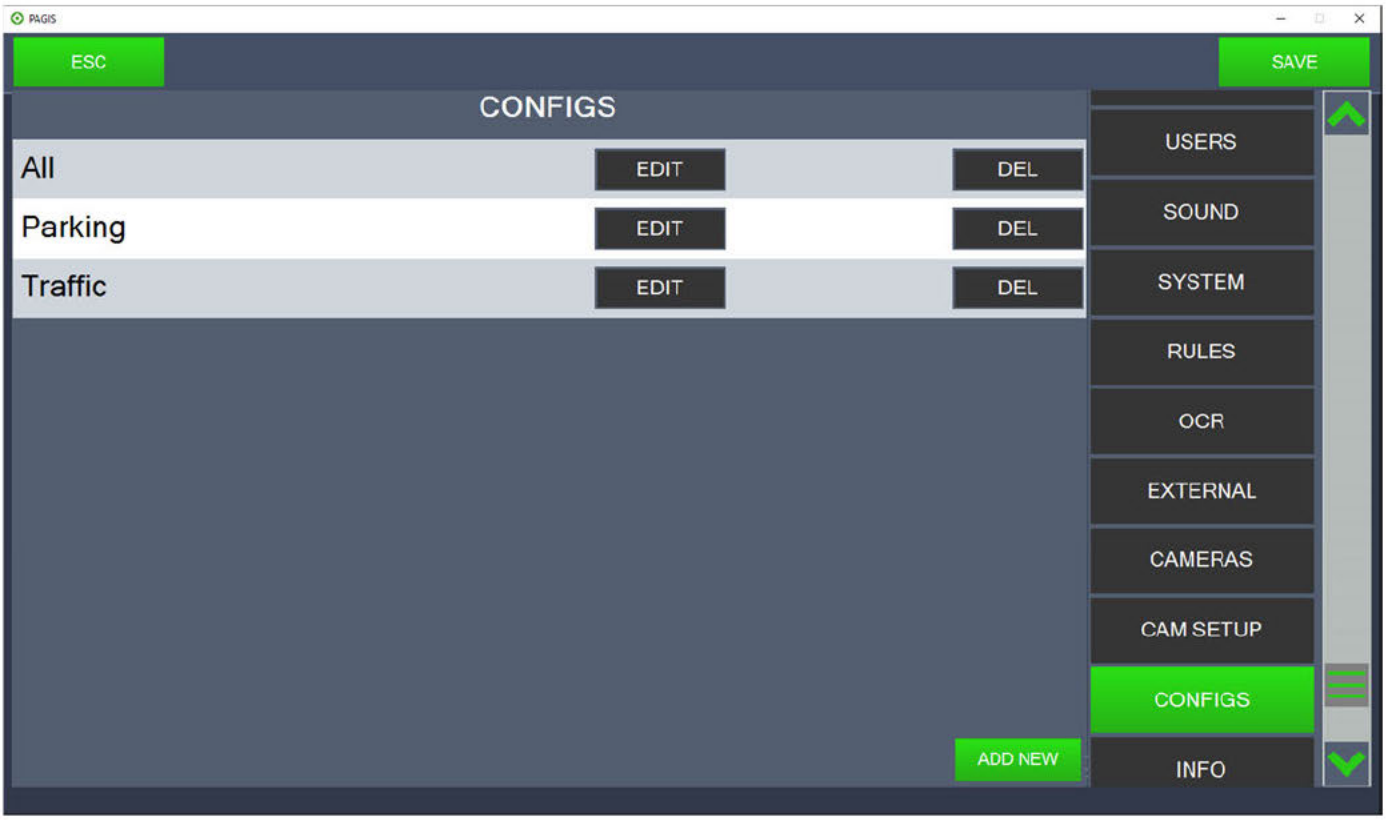


IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button

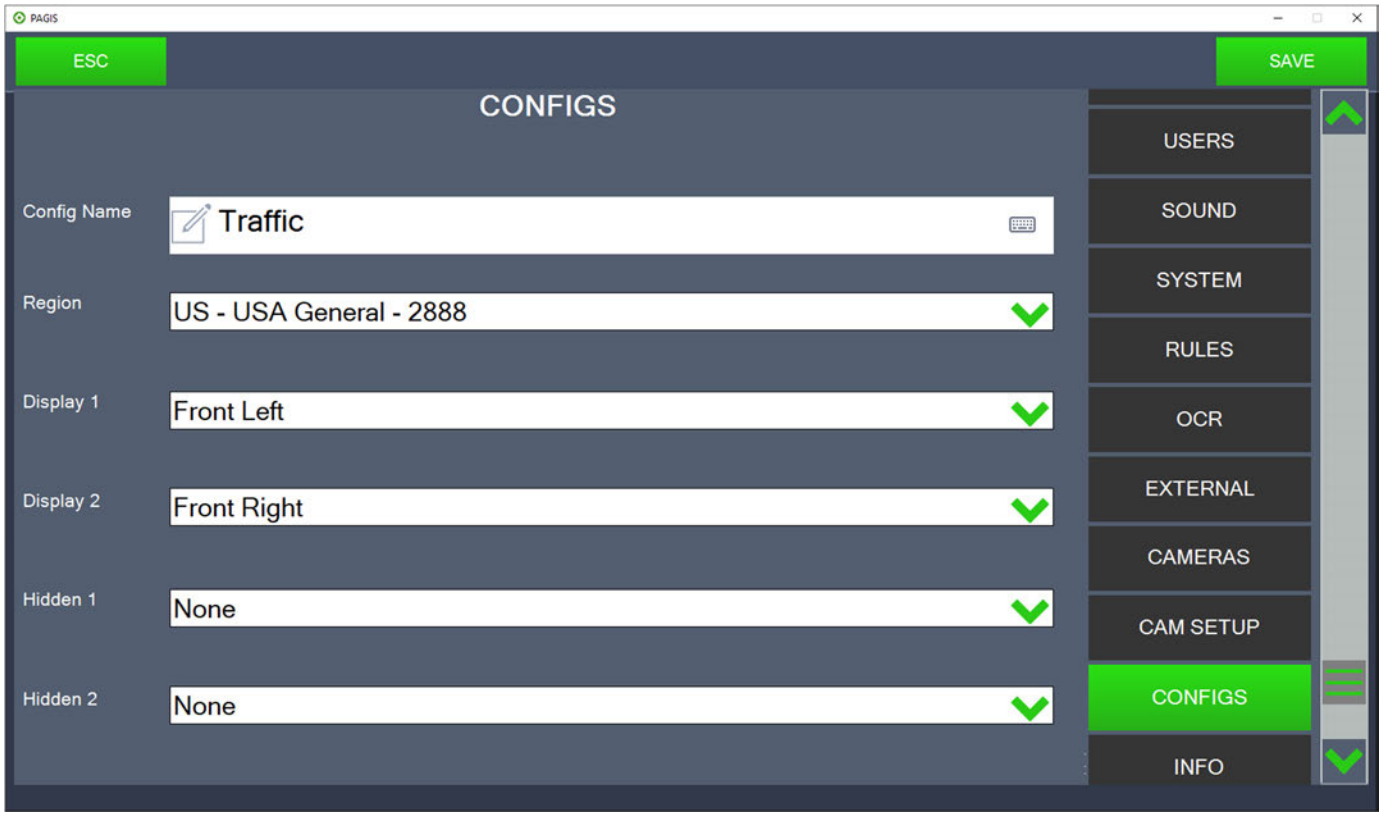


To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.

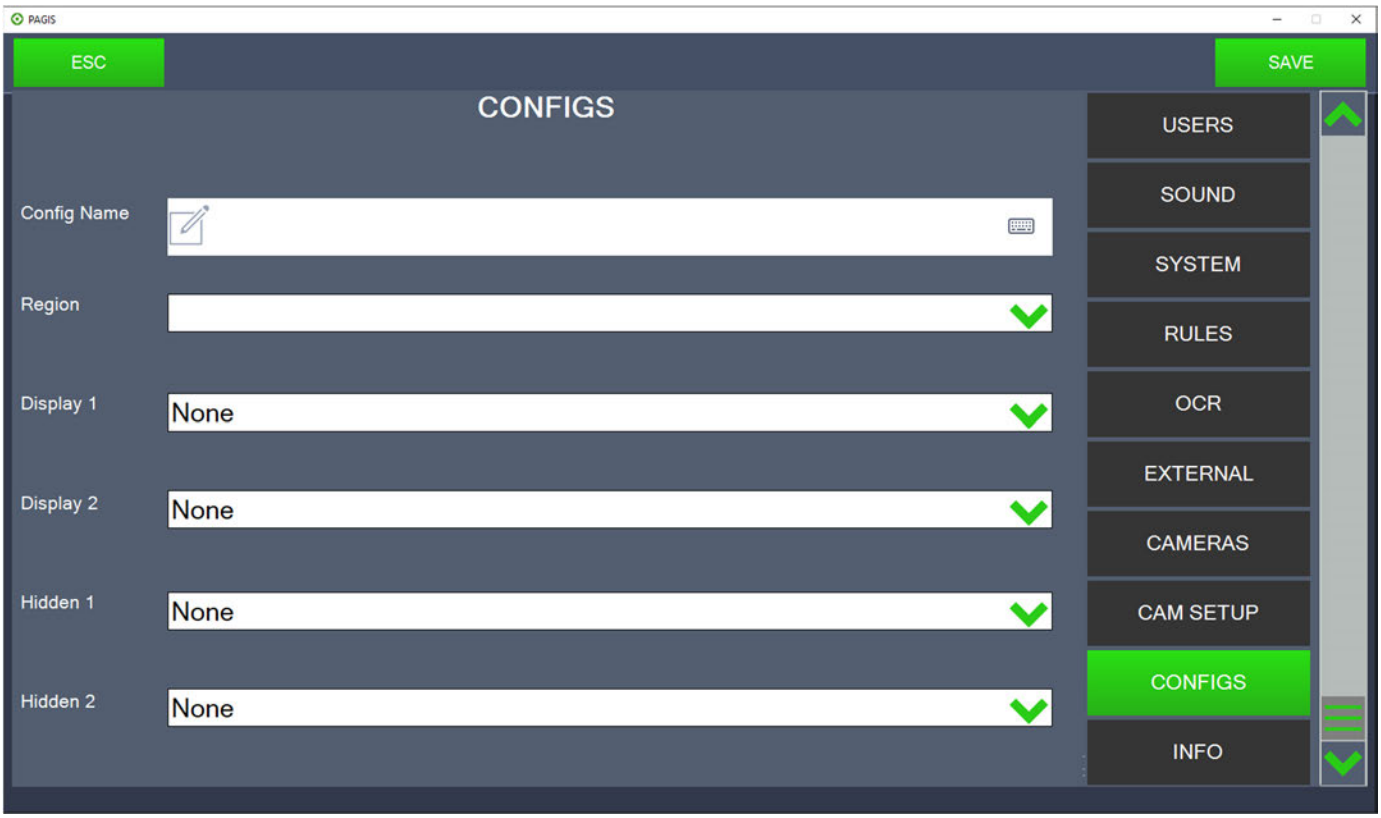


1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info

1034

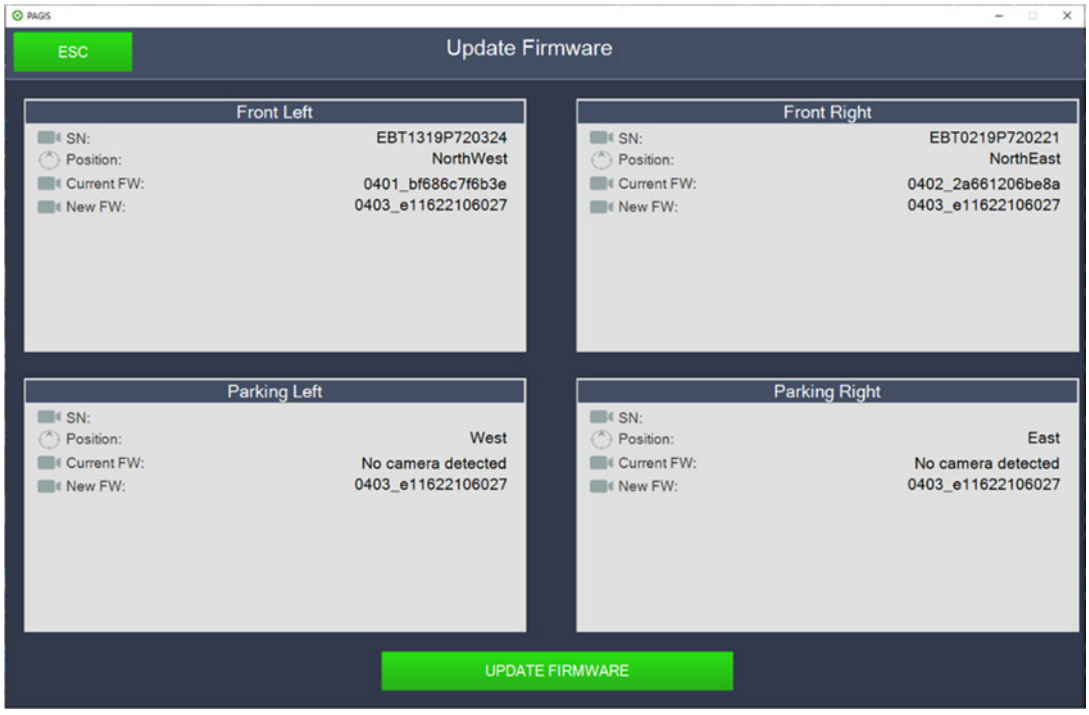
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The PIPS mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the PIPS mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the PIPS processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the .200 IP address, using alternative IP’s on Laptops will result in the software’s failure to communicate with the cameras.

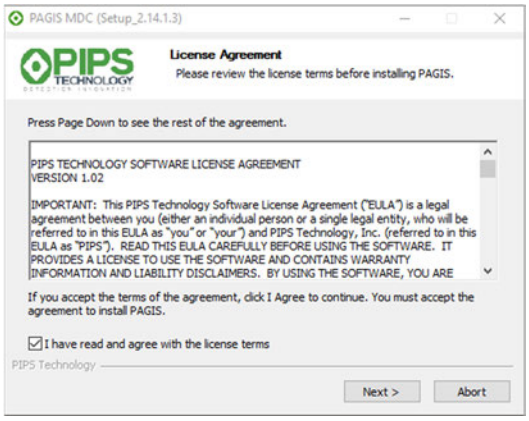
4.2.2 PAGIS Software Installation (MDC)

1036

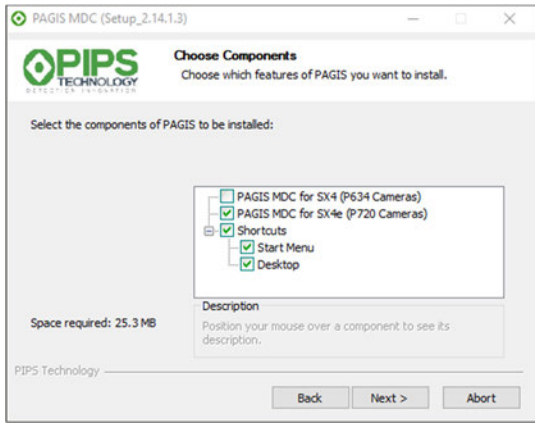
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor, if the 4 camera IO ports are vertically arranged RJ45’s then it’s a SX4e, if they are vertically arranged circular shaped “LEMO” connectors then it’s a SX4. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. When upgrading to PAGIS V2.14.x.x also requires that the PIPS mobile processor be updated to same version in order to take advantage of Firmware update.



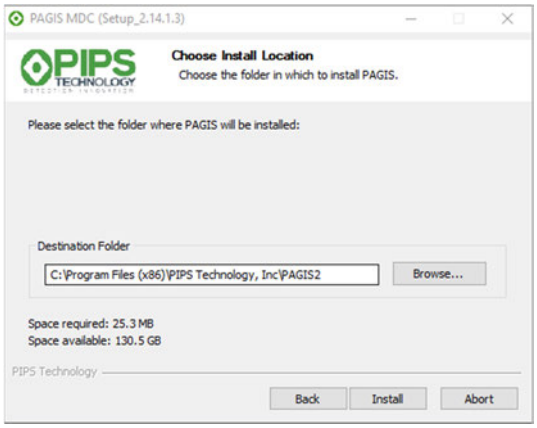
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



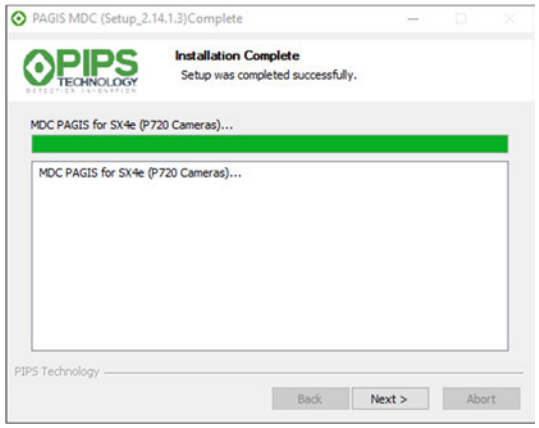
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

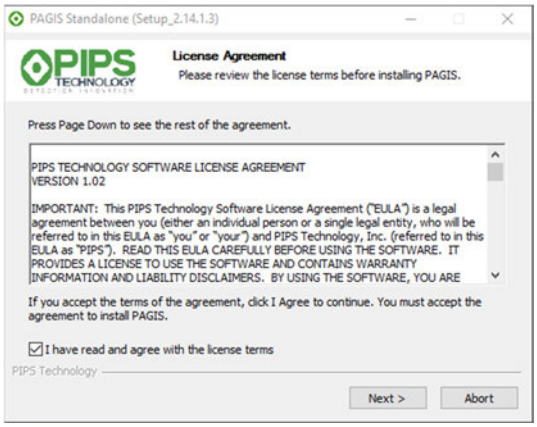
Note: See Appendix A for terminology definitions.

4.2.3 PAGIS Software Installation (Mobile Processor)

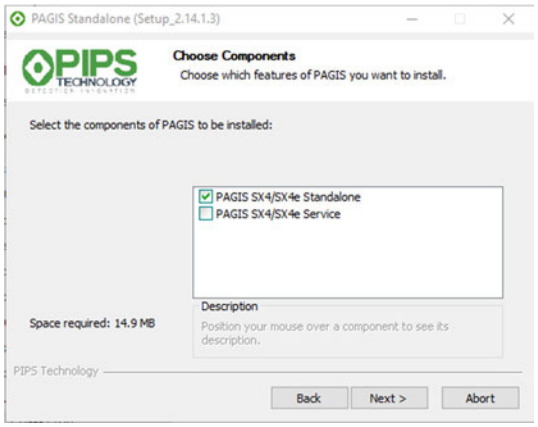
1. PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.



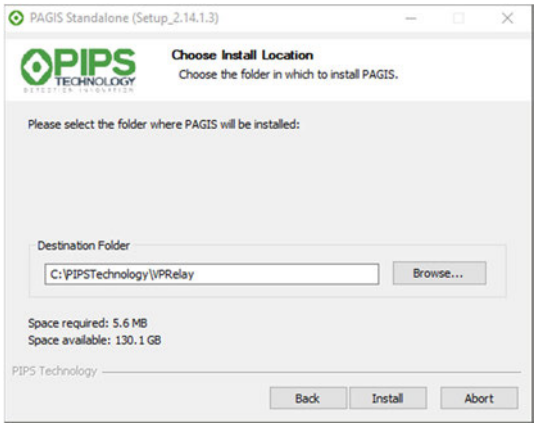
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



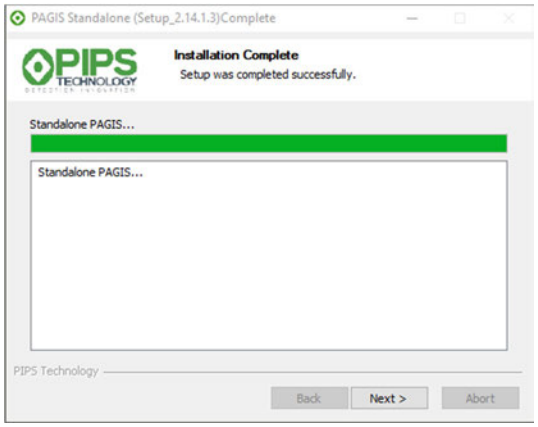
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

PAGIS/BOSS3 CONFIGURATION 1039

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device. **NOTE**: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the “Hotlists” button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the “Deployment” field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be “built” or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating “HttpStatusCode” will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

1042

ALPR/ANPR	“Automatic License Plate Recognition/Automatic Number Plate Recognition”.
BOSS	“Back Office System Software”. This is the ALPR server.
GPS	“Global Positioning System”.
GUI	“Graphical User Interface”.
Hotlist	A database or list that contains vehicle license plates of interest (“alert list”).
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	“Mobile Data Computer”. This is the tablet or laptop in the vehicle.
OCR	“Optical Character Recognition” (also referred to as a “cardet”).
OS	“Operating System”.
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or “VPRelay” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface. Same a “Service”
SX	SX is a short notation referencing PIPS’s mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A “User Interface” is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	“Vehicle License Plate”.
VPN	“Virtually Protected Network”.
VPRelay	Operation mode of the PAGIS software. VPRelay or “Service” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of

the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors. [1046]

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for

help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**

Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**

A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

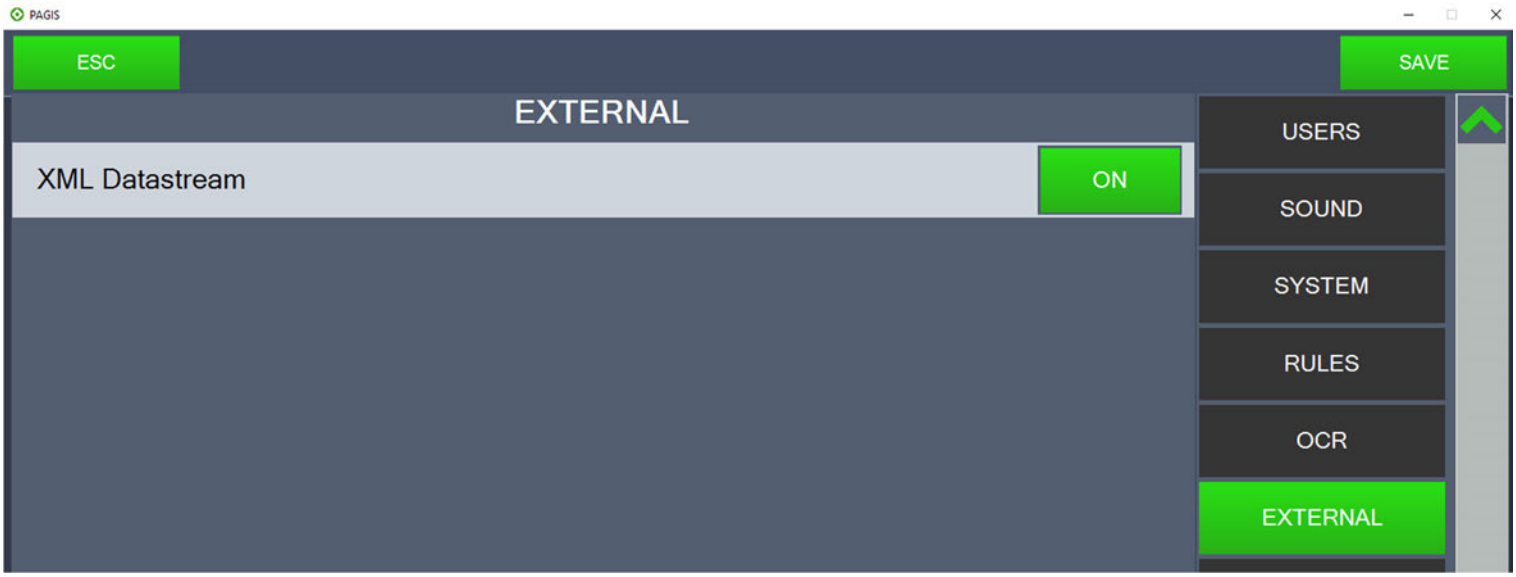
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "YYYY-MM-DDThh:mm:ss".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD..................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS User's Manual

Version 2.14

Updated 3/30/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 3

Technical Support 3

Design Changes 3

Trademarks 3

Copyright 3

Version 3

INTRODUCTION 4

1.1 Dual Lens Color and Infrared Camera 4

1.1.1 Available Products 4

1.2 Using This Manual 5

SCREEN REFERENCE 6

2.1 The PAGIS Software Login Screen 6

2.1.1 Logging on with the Default Administrative Account 6

2.2 Main Screen - Live View 7

2.2.1 Getting Started in PAGIS 7

2.3 The PAGIS Navigation Buttons 8

2.3.1 Camera Control Buttons 8

2.3.2 GPS Indicators 9

2.3.3 Camera Firmware Update (Restricted Users) 9

2.3.4 Day/Night Mode 9

2.4 Begin Shift 10

2.4.1 Sync via USB Thumb drive (or Local Source) 10

2.4.2 Sync via Wireless Network 10

2.4.3 PAGIS Auto-Sync Settings 10

2.4.4 Begin Shift – Additional Information 10

2.5 End Shift 10

2.5.1 Sync to BOSS 10

2.6 Cam Mode Button 11

2.6.1 Camera Modes 11

2.7 Taking a Picture 11

2.8 Search Entry Screen 12

2.8.1 Searching Synchronized Hotlists for License Plates 12

2.8.2 Searching Locally Stored Reads and Hits 12

2.8.2.1 Searching for a Match 13

2.8.3 Wild Card Symbols 13

2.8.4 Manually Adding a Plate to PAGIS 14

2.8.4.1 ADD VLP Query 14

2.8.4.2 ADD VRM Report Screen 14

2.9 The Review Screen 15

2.9.1 Summary Review Section 15

2.9.2 Review Navigation Buttons 15

2.9.3 Reads 16

2.9.3.1 Reads Result Screen Navigation Buttons 16

2.9.3.2 Interactive Buttons – Reads Screen 16

2.9.4 Hits 17

2.9.4.1 Hit Screen Attributes 17

2.9.4.2 Hit Screen Function Buttons 18

2.9.4.3 Interactive Buttons – Hits Screen 18

2.9.4.4 Set Disposition – Additional Detail 18

2.9.4.5 Add Intel – Additional Detail 19

2.9.5 Misreads 19

2.9.5.1 Marking a Record as a Misread: 20

2.9.6 Audits 21

2.9.7 Targets 21

2.9.7.1 The Targets Screen 22

2.9.7.2 Targets Screen Navigation Buttons 22

2.9.8 Databases 23

2.9.8.1 Databases Screen Functions 23

2.9.8.2 Databases Screen Navigation Buttons 23

2.9.8.3 Databases Edit- “Manual Reports” 24

TROUBLESHOOTING TIPS 25

3.1 Troubleshooting & Tips 25

3.1.1 PAGIS with NetMotion VPN 25

3.1.2 Cisco VPN Client: 25

3.1.3 Microsoft .NET 3.5 Installation 25

3.1.4 Firewall Settings for Client-Server Installations 25

APPENDIX A: THE GLOSSARY 26

APPENDIX B: PAGIS SOFTWARE DATABASE FILE 27

APPENDIX C: FAQ 29

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

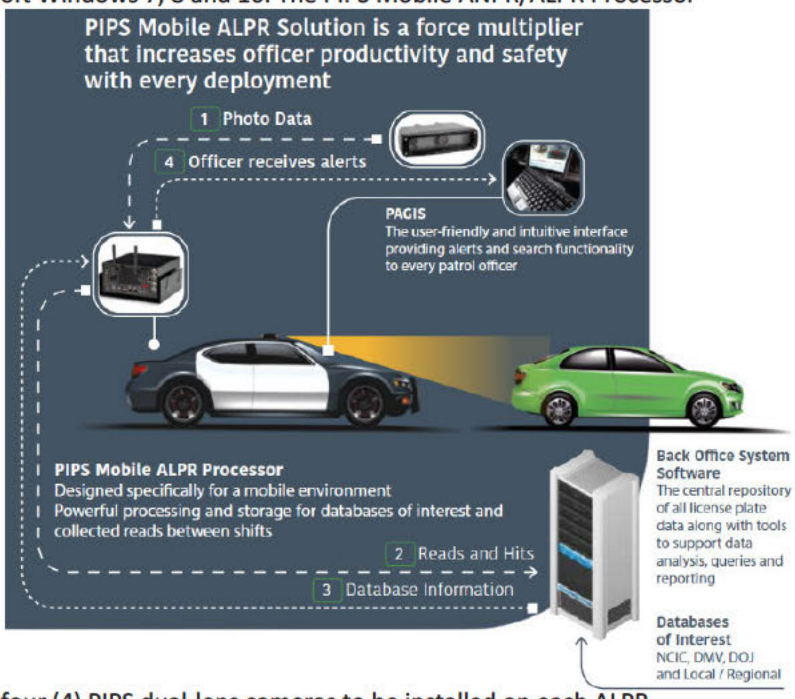
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

1057

The section overview of this software manual are as follows:

Section 1: The Introduction and Basics

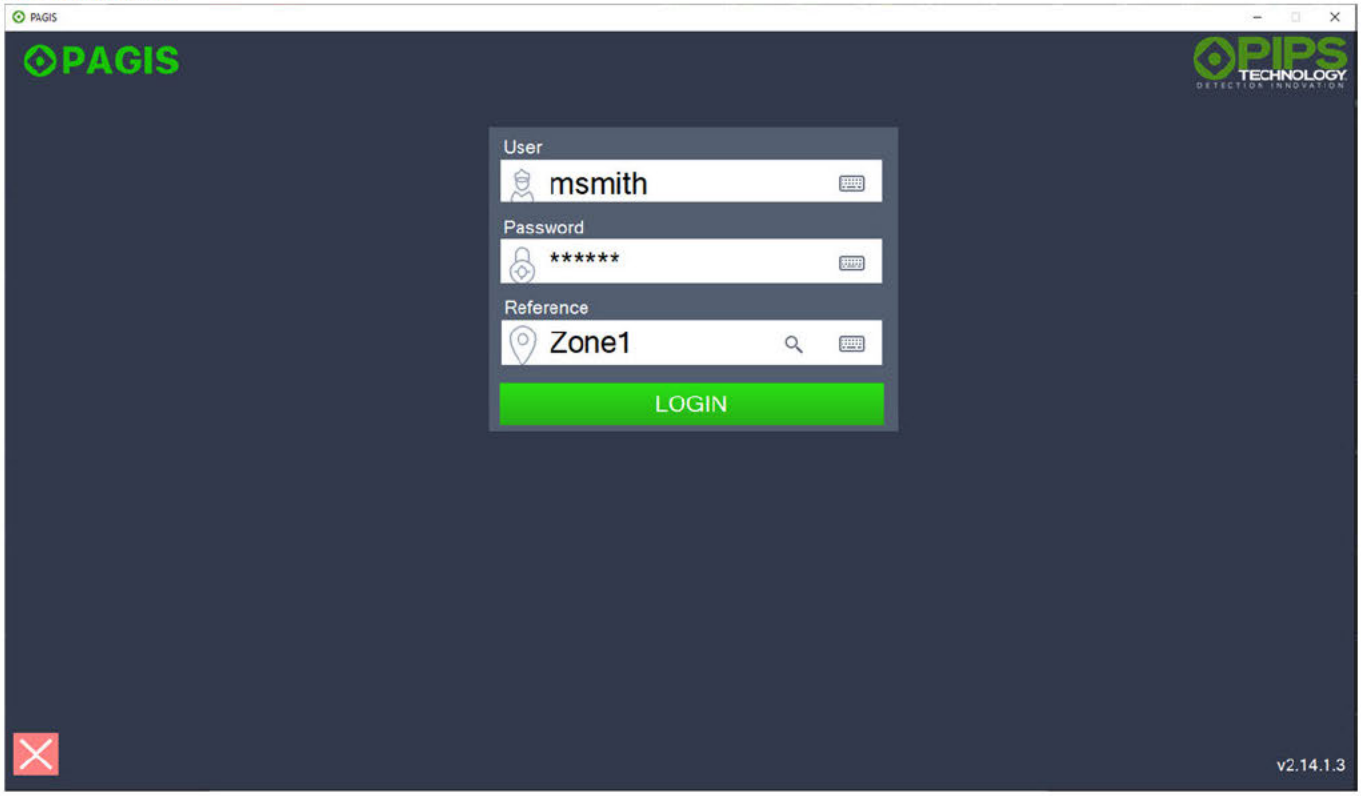
Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

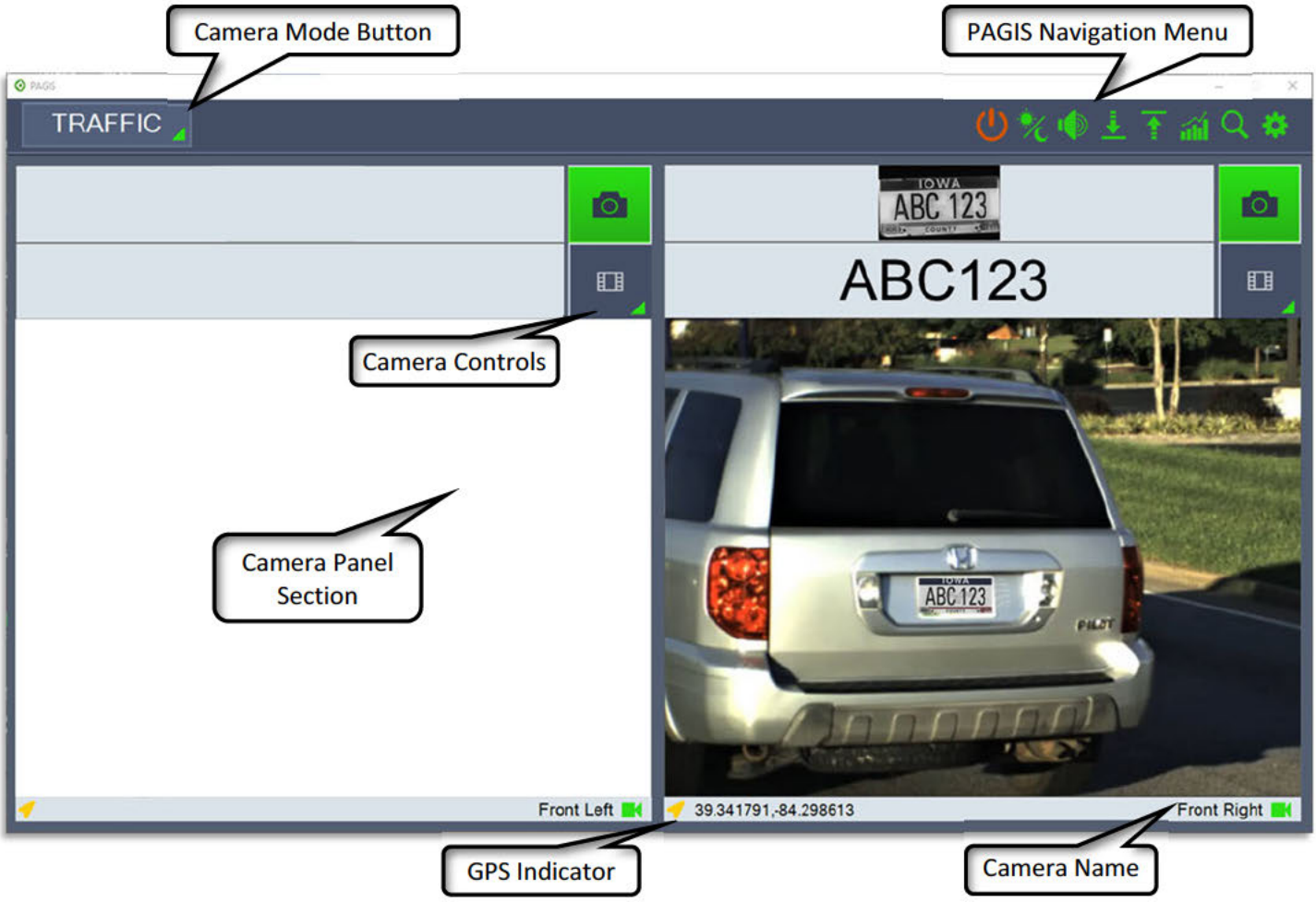
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

1060

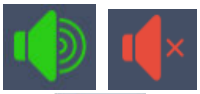
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

1061

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

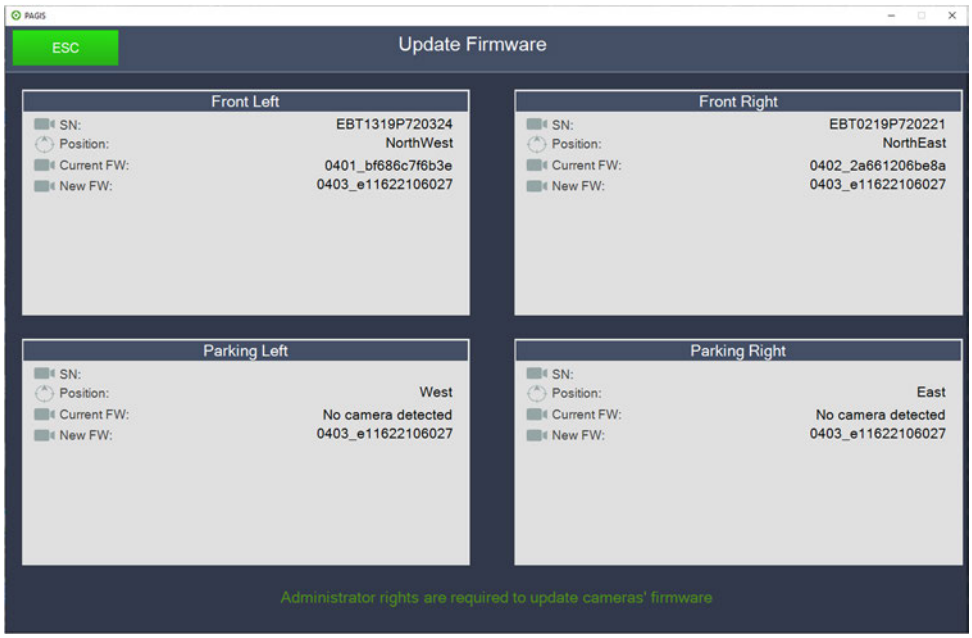
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

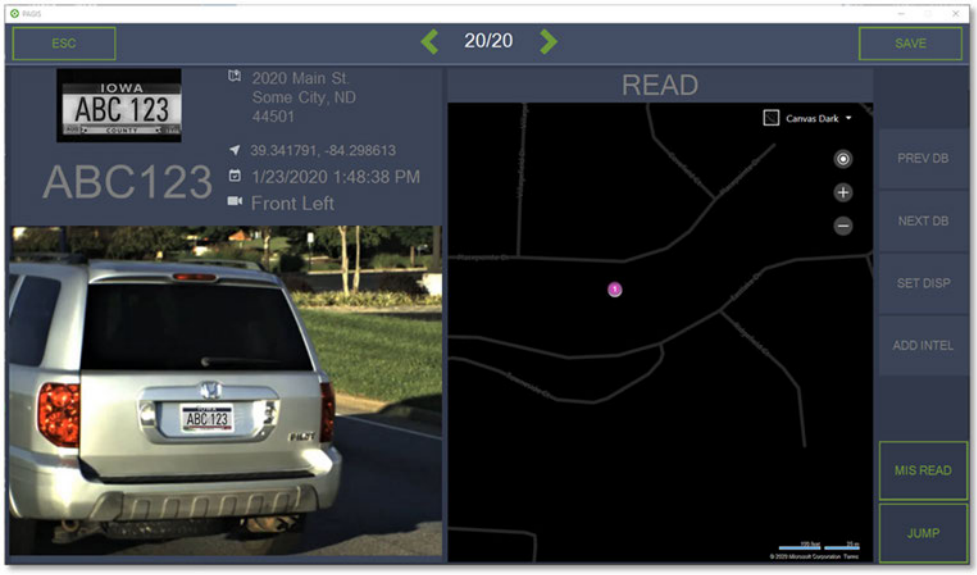


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

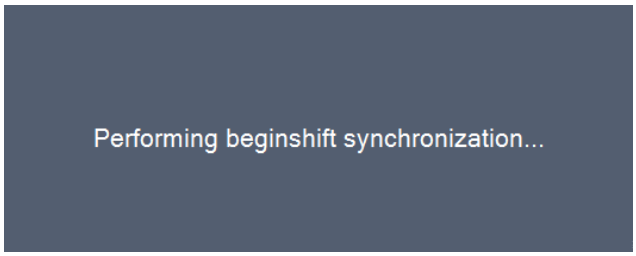
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

NOTE: The picture will Not be saved if a description/note is not entered in the text box.

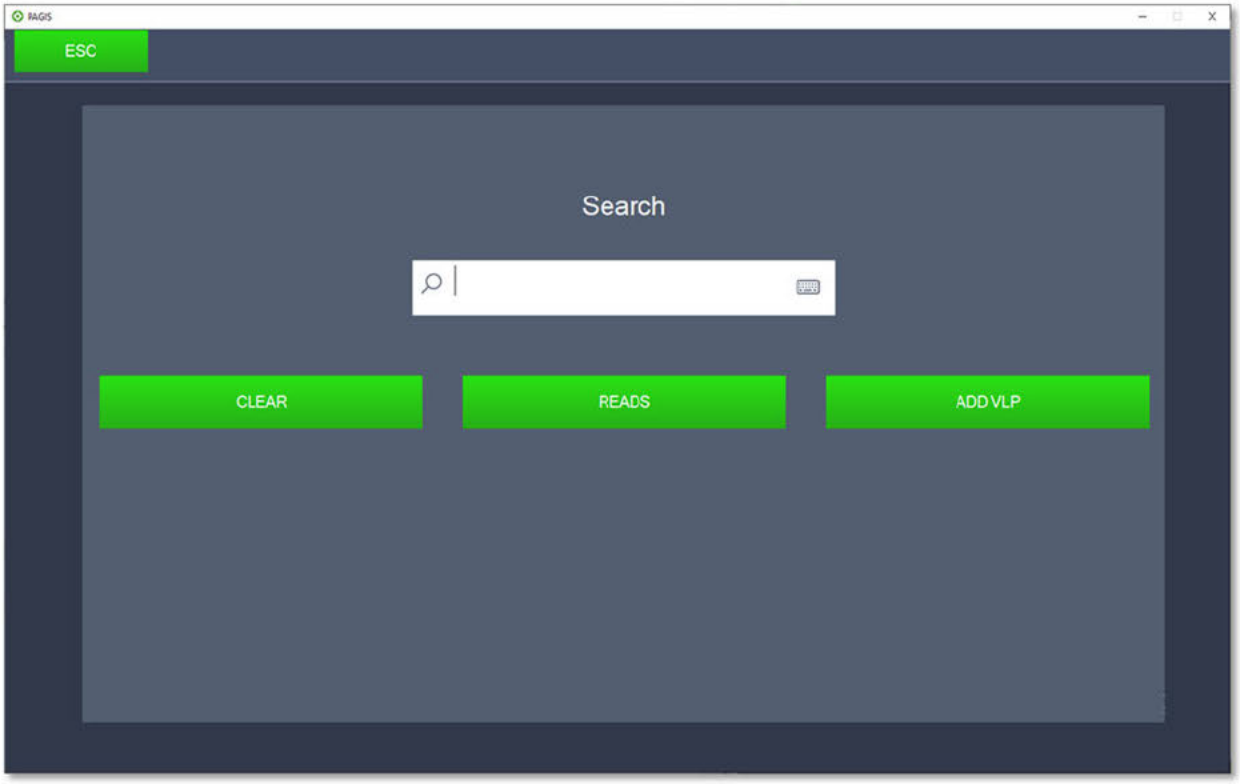
To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

1064

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

1065

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

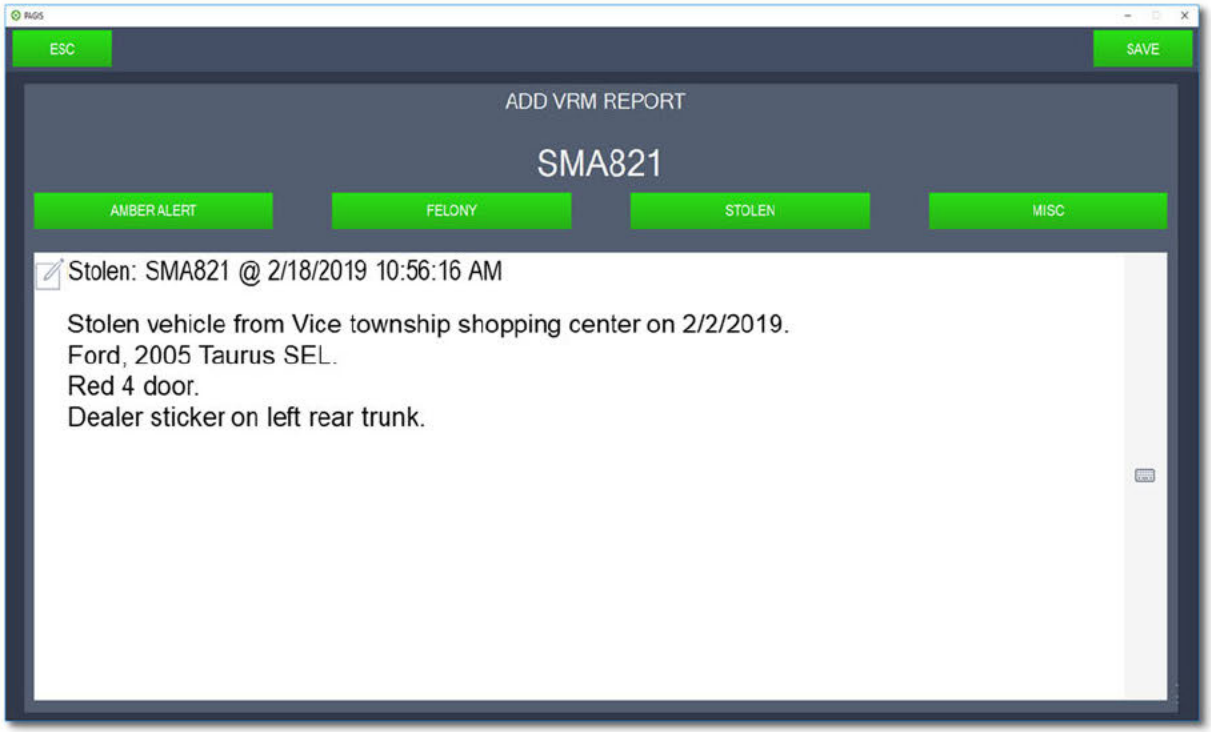
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

1067

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

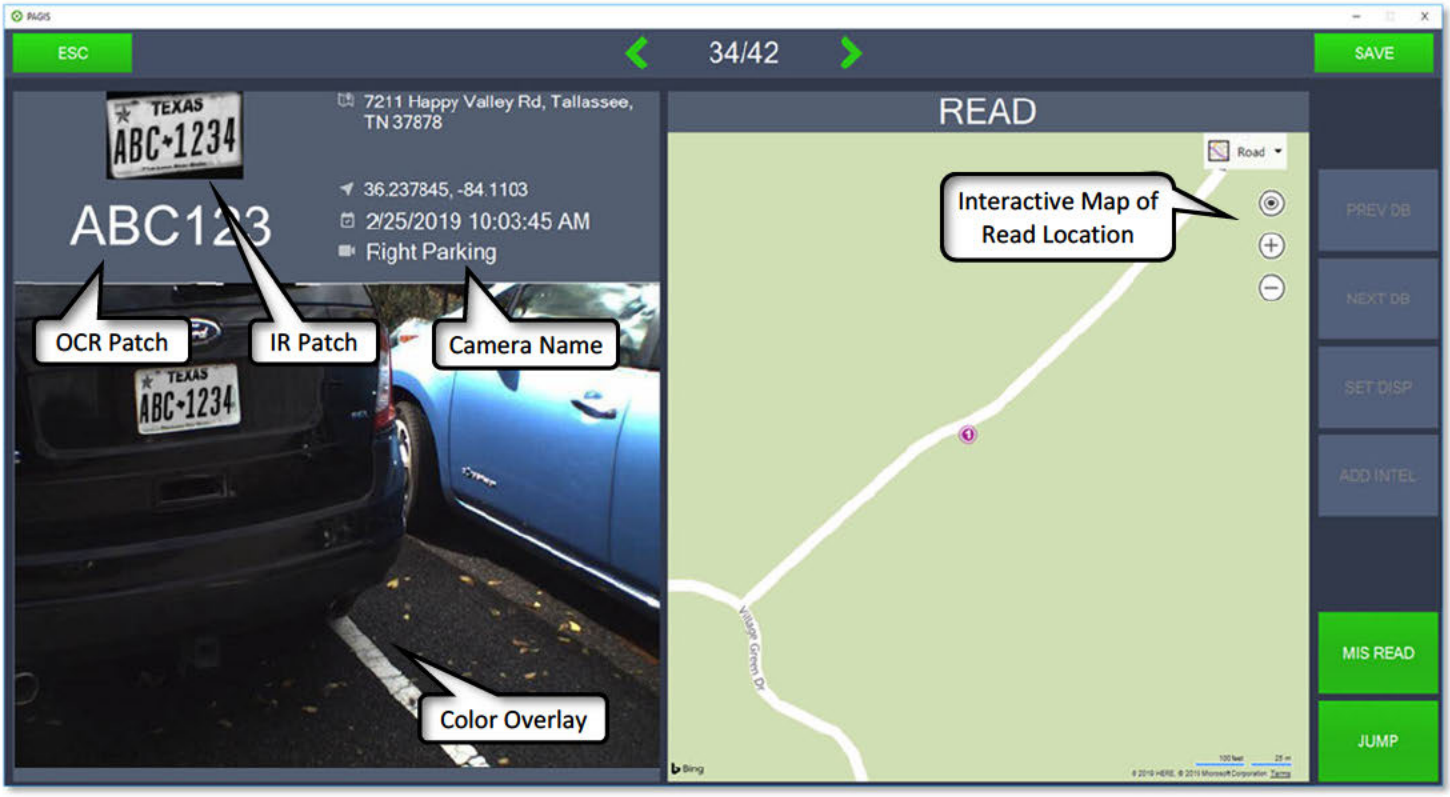
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

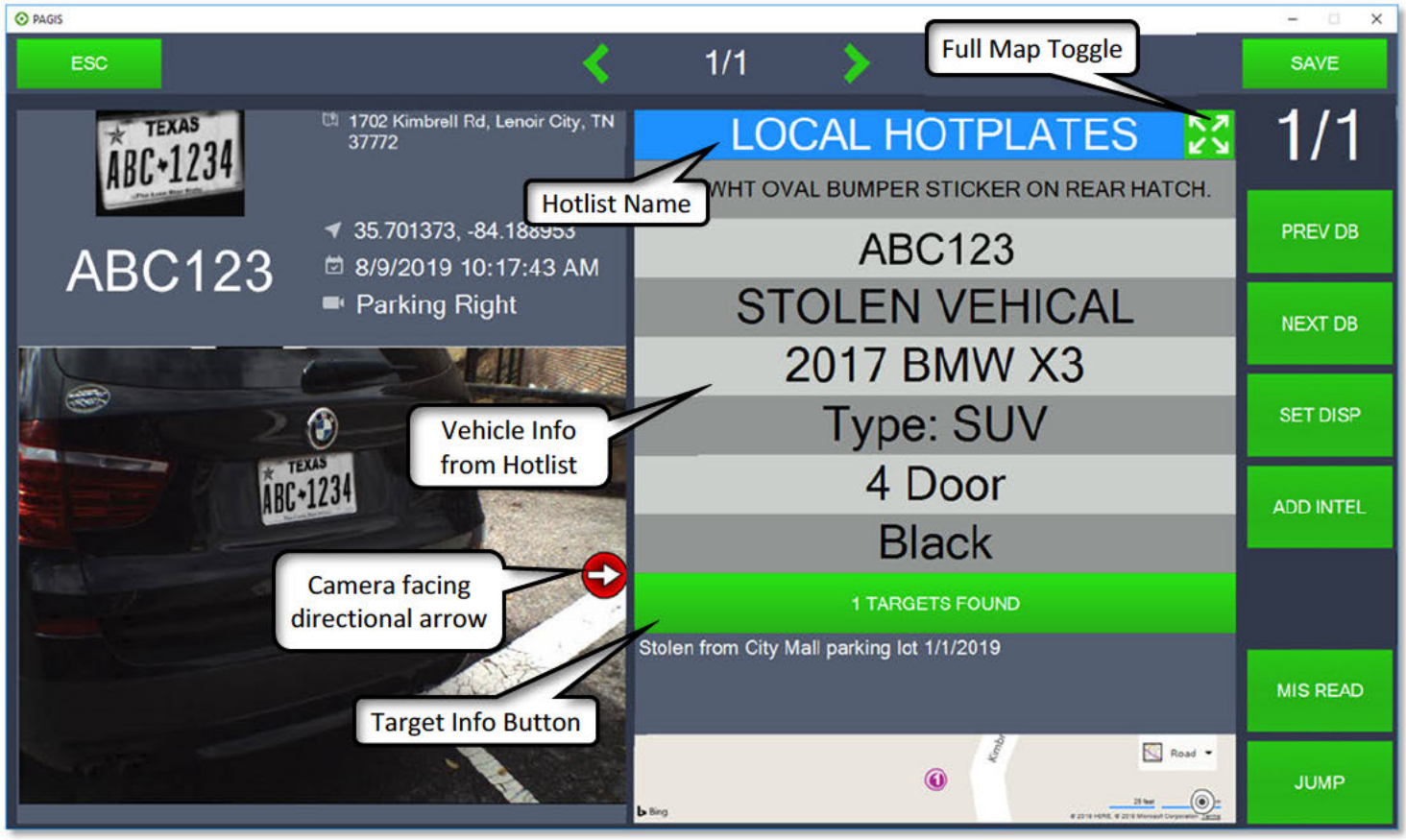
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

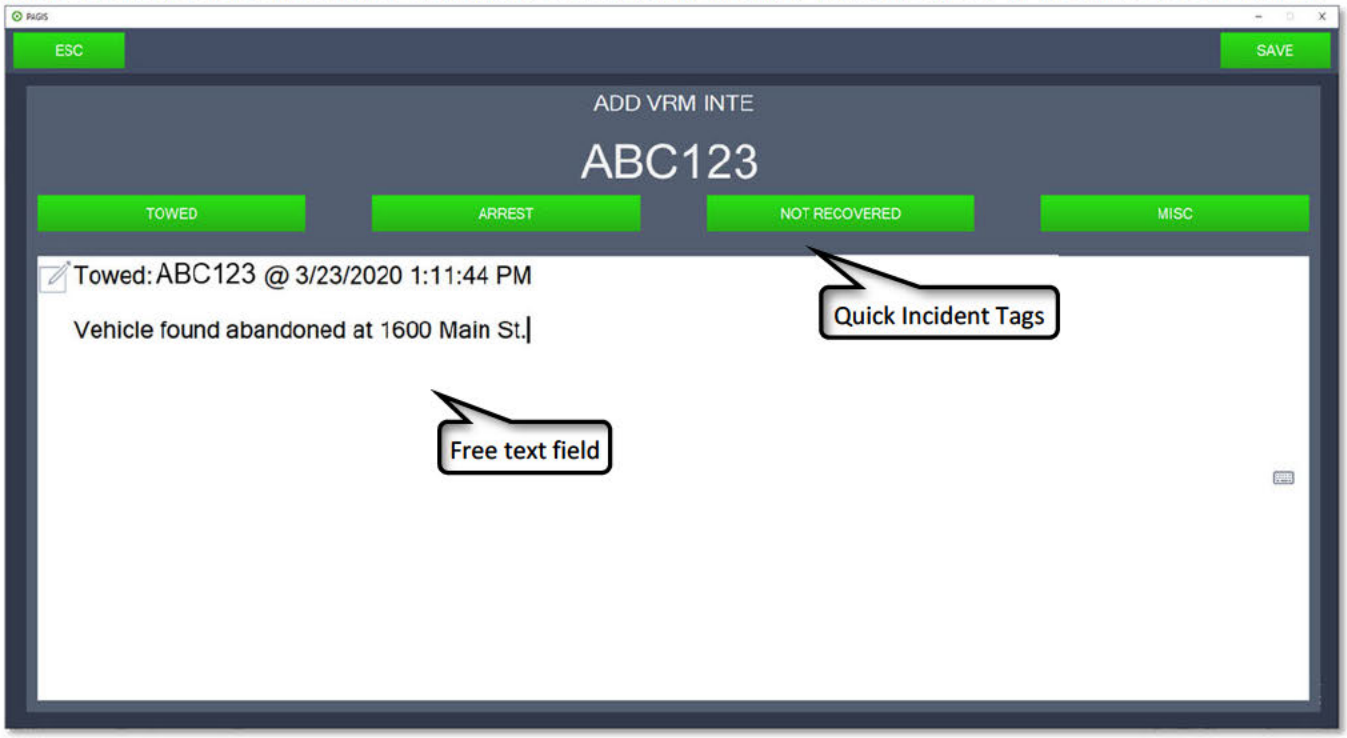


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

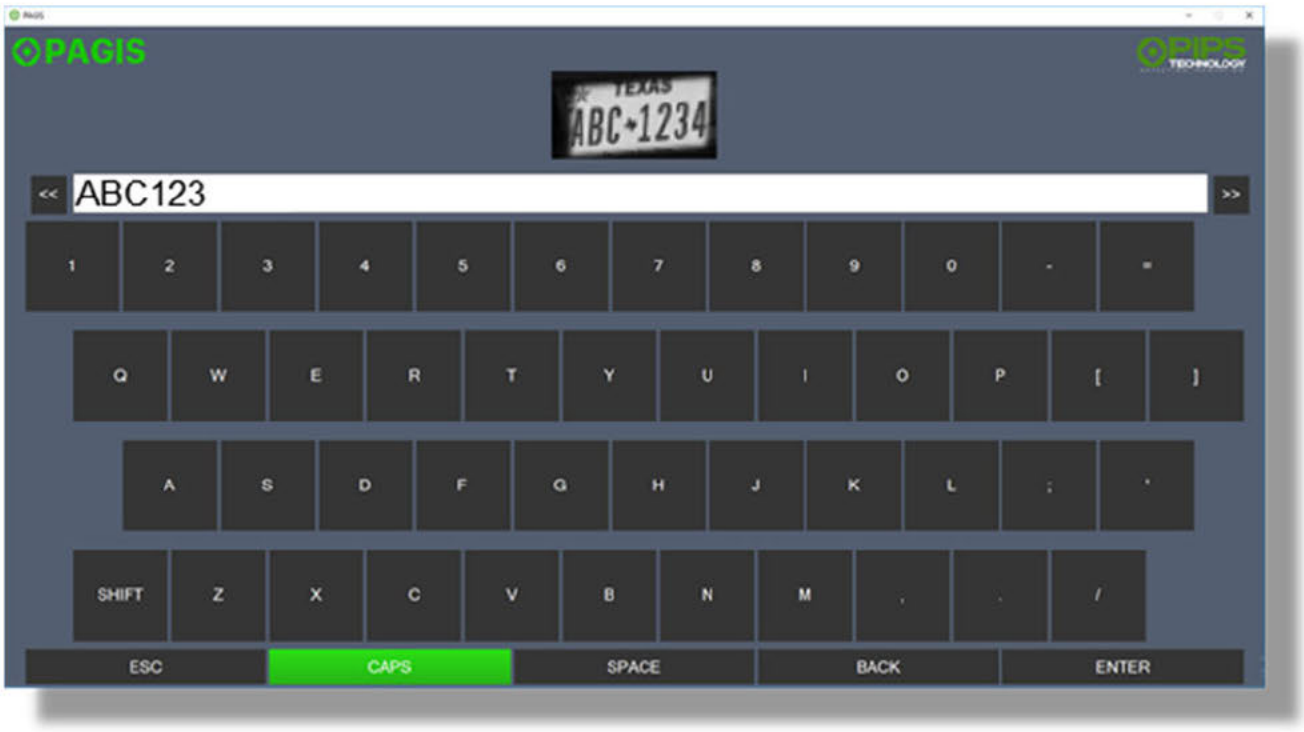
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

Updating the Read/Hit OCR Patch:

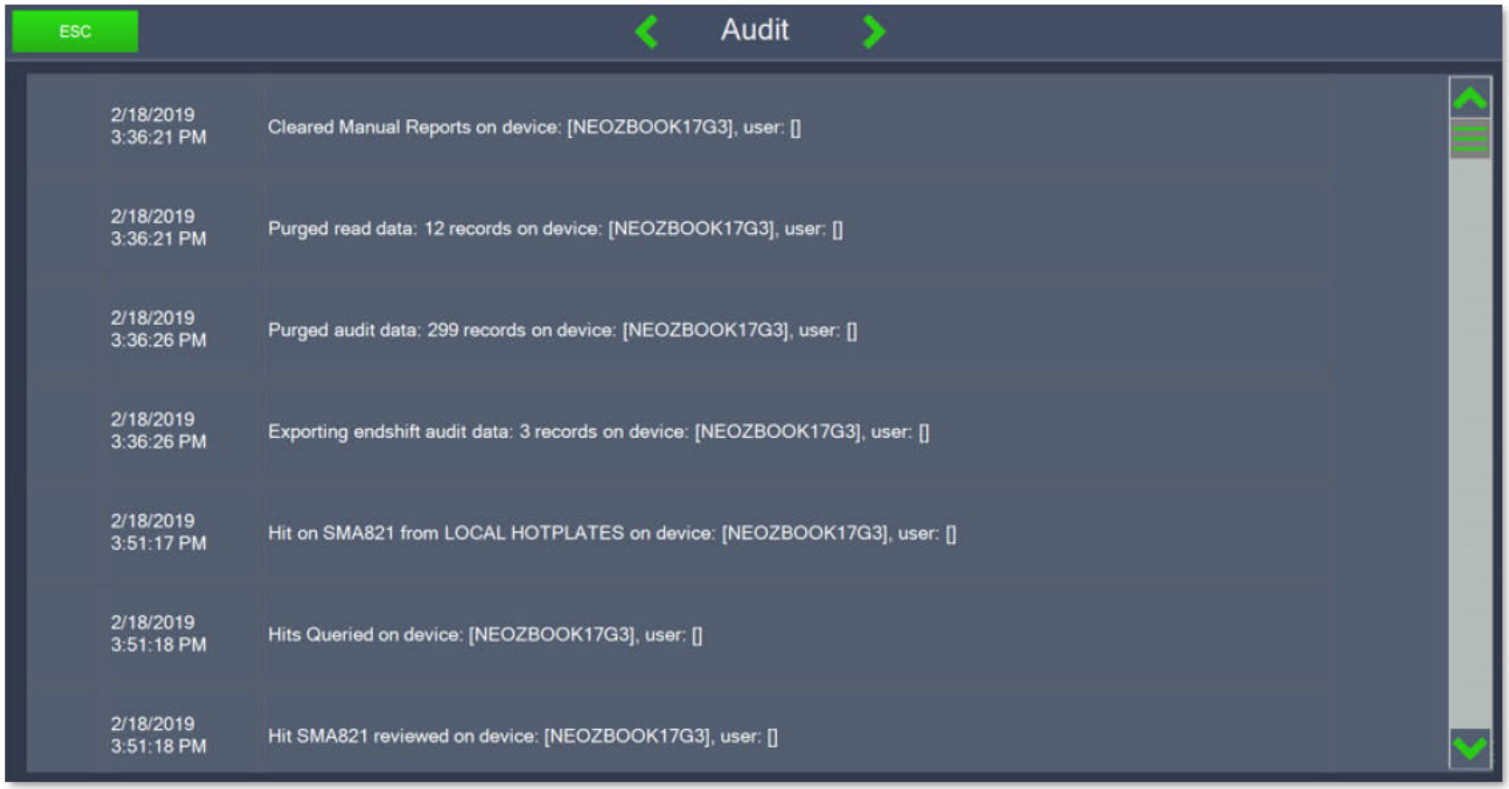
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

1073

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



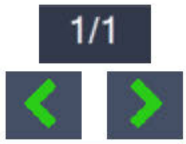
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

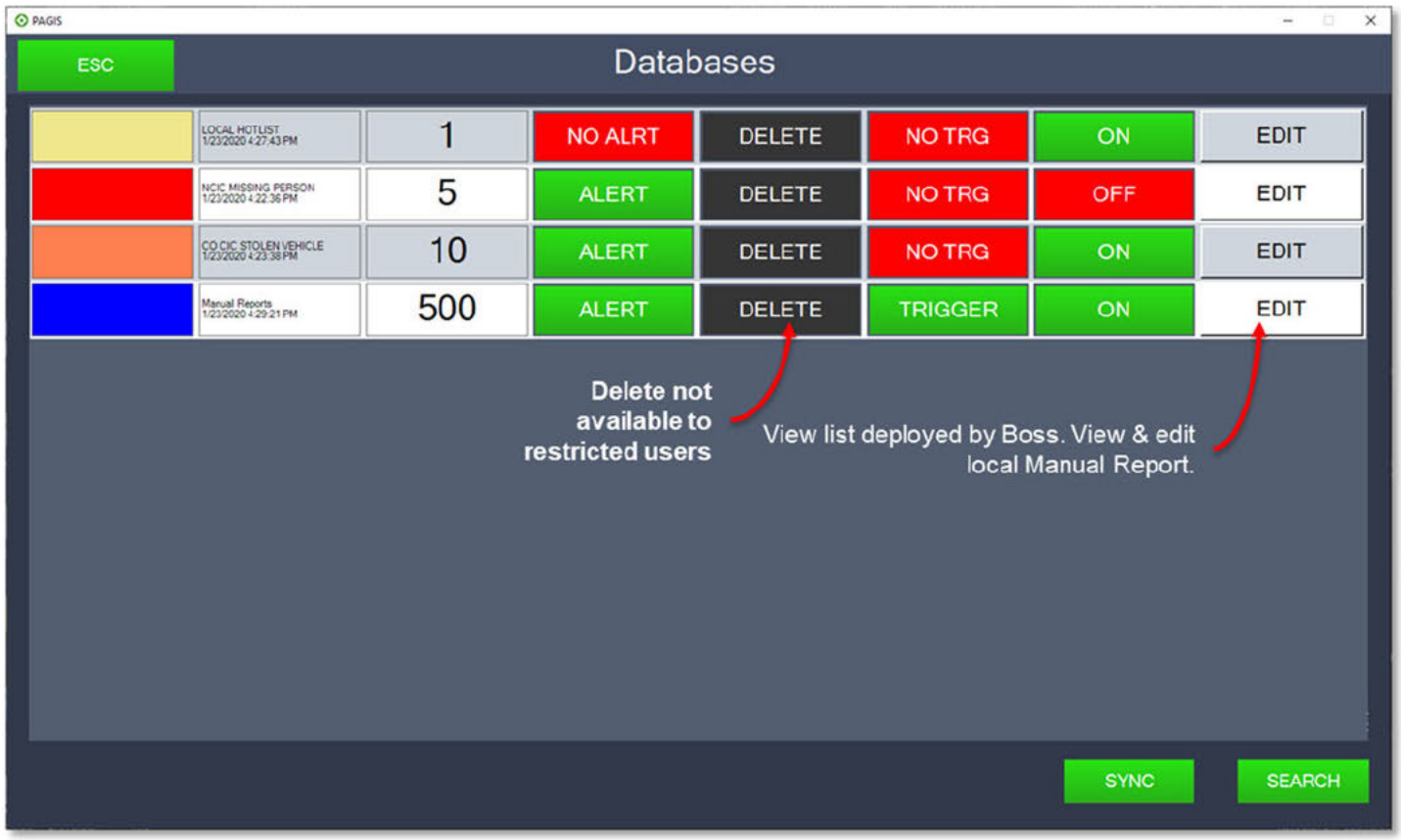


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

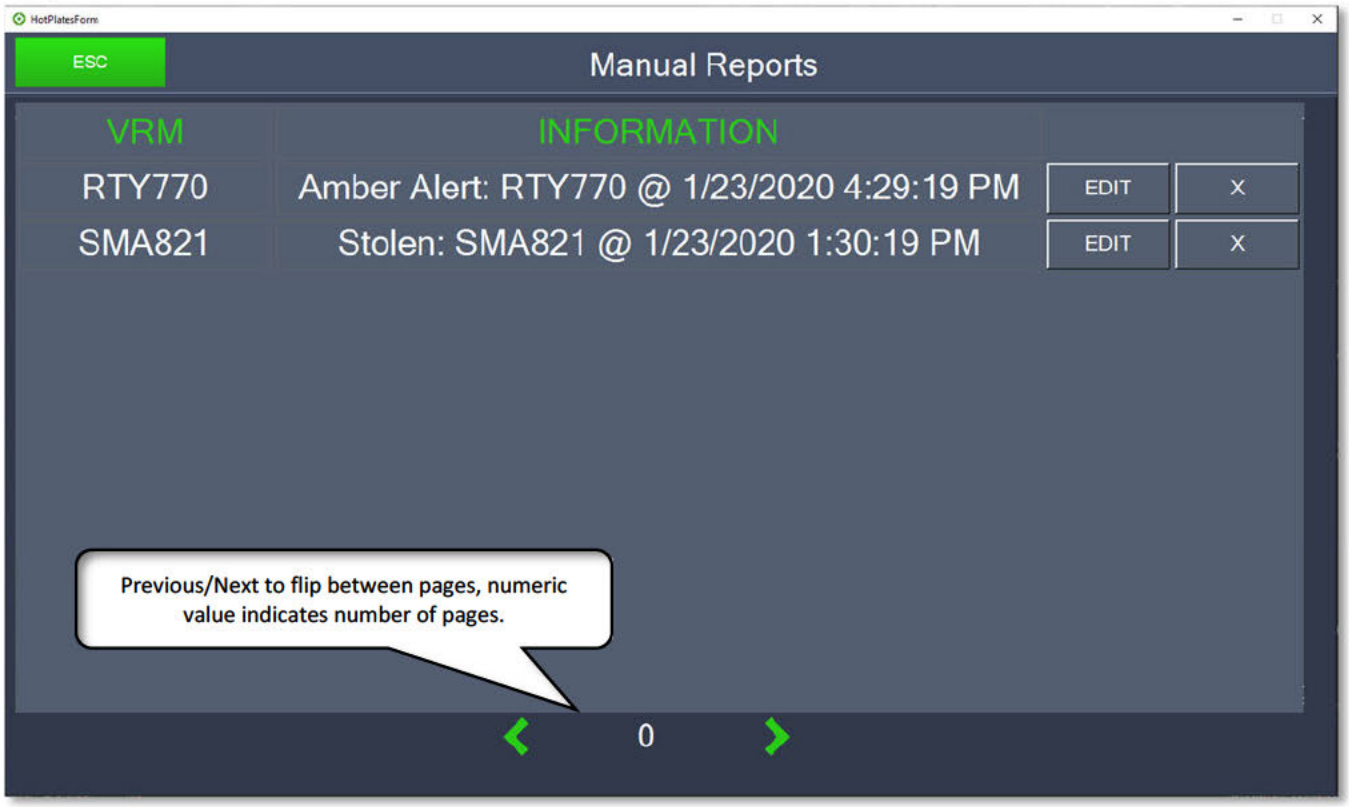
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

3.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

3.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

3.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

3.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

3.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall.

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: “C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe”

Option 3: Add the communication ports manually:
TCP 8092
TCP 9000
TCP 9001
TCP 32023
TCP 32029
TCP 10000
TCP 10010
NOTE: XML Datastream uses TCP 10100 and TCP 7000

APPENDIX A: THE GLOSSARY

ALPR/ANPR	“Automatic License Plate Recognition/Automatic Number Plate Recognition”.
BOSS	“Back Office System Software”. This is the ALPR server.
GPS	“Global Positioning System”.
GUI	“Graphical User Interface”.
Hotlist	A database or list that contains vehicle license plates of interest (“alert list”).
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	“Mobile Data Computer”. This is the tablet or laptop in the vehicle.
OCR	“Optical Character Recognition” (also referred to as a “cardet”).
OS	“Operating System”.
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or “VPRelay” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface.
SX	SX is a short notation referencing PIPS’s mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A “User Interface” is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	“Vehicle License Plate”.
VPN	“Virtually Protected Network”.
VPRelay	Operation mode of the PAGIS software. VPRelay or “Service” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE[1079] DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE HAVE NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the

Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."

Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left camera to the Right camera position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

neology™
mobility [re]imagined™

Police ALPR Graphical Interface Software (PAGIS)

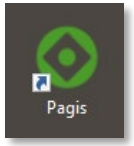
User / Admin Training

Presenter: Michael Roth

PAGIS Ver. 2.14

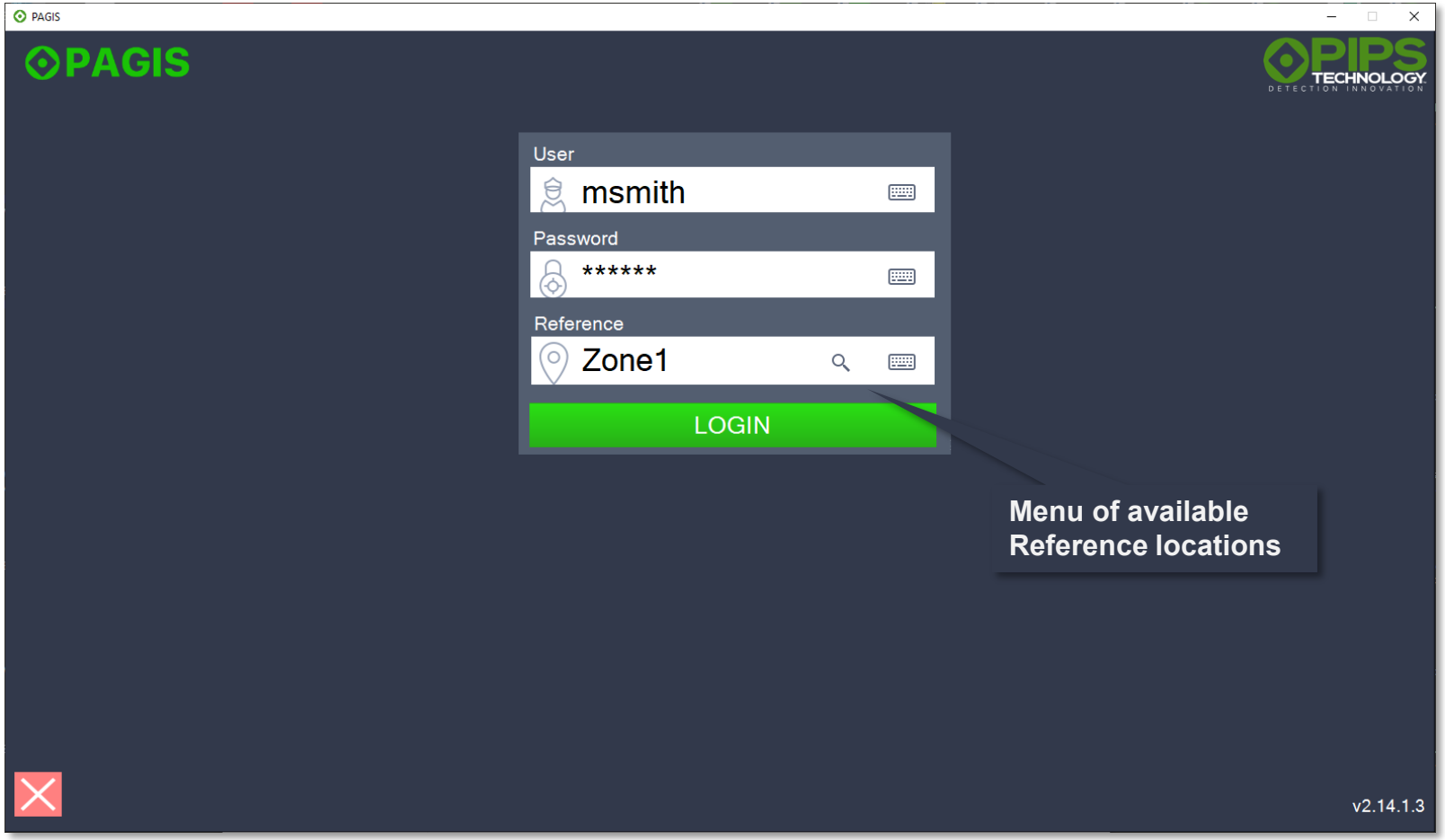
4/21/21

Starting PAGIS



To start, double click the **PAGIS** icon on desktop.

- **User-** Enter assigned username.
- **Password-** Enter password. Depending on Boss setting this may or may not be required.
- **Reference-** Select or Enter department, location or activity specific reference. Each license plate Read will have this label associated with it when the field is populated, this field can be used as an additional search filter to sort data in BOSS.
- **KeyPad-** Available throughout PAGIS where keyboard symbol is present.
- **LOGIN-** Initiate login.

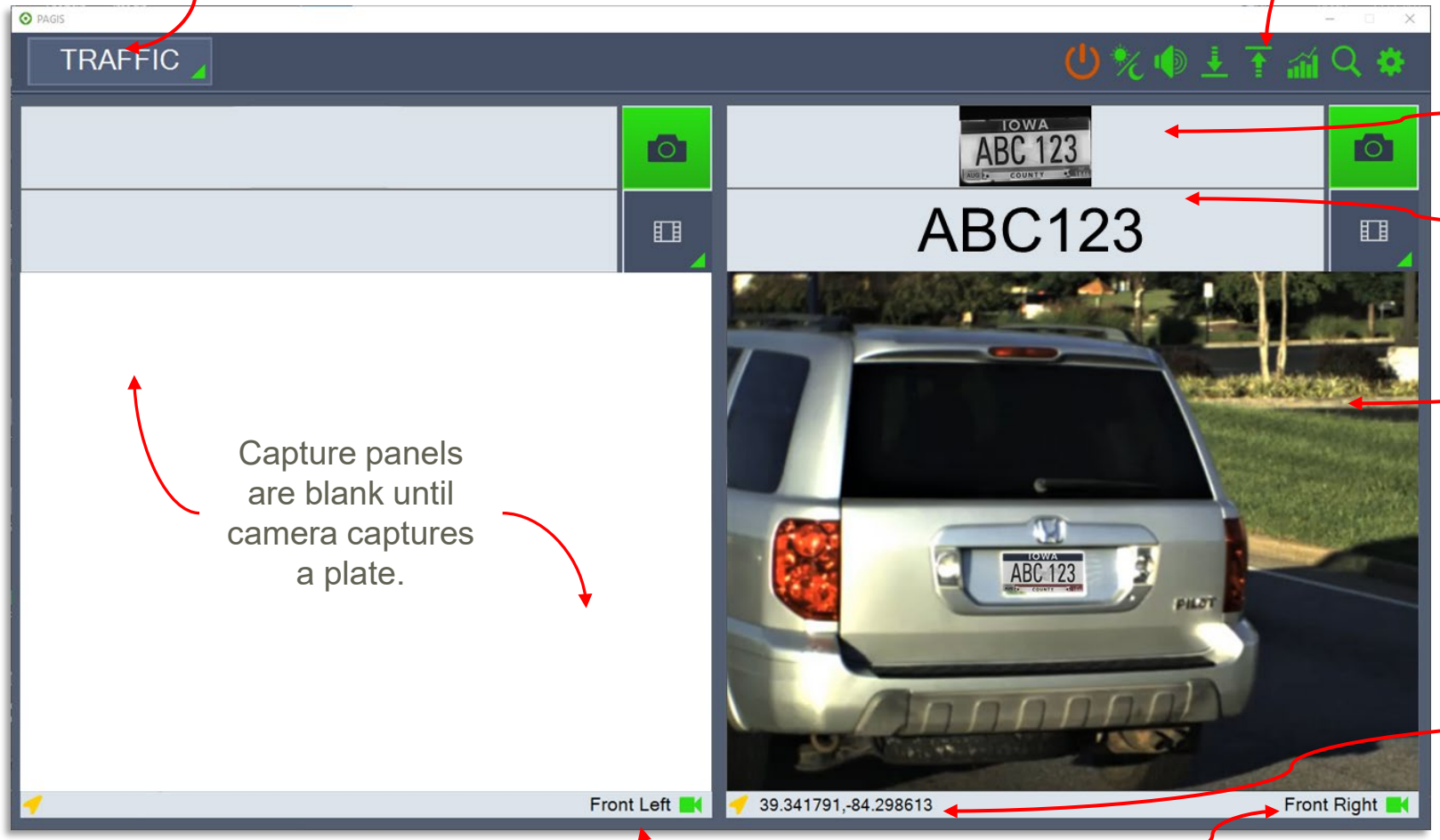


Copyright © 2021 Neology, All Rights Reserved.

Main View Screen

PAGIS defaults to two Camera Display Panels. “Cam Mode” controls what's currently being displayed on screen.

PAGIS System Control Features.



Infrared plate patch
(IR plate Read or “patch”)

OCR text translation of IR plate patch.

Color Overview
Captures are displayed as static images.

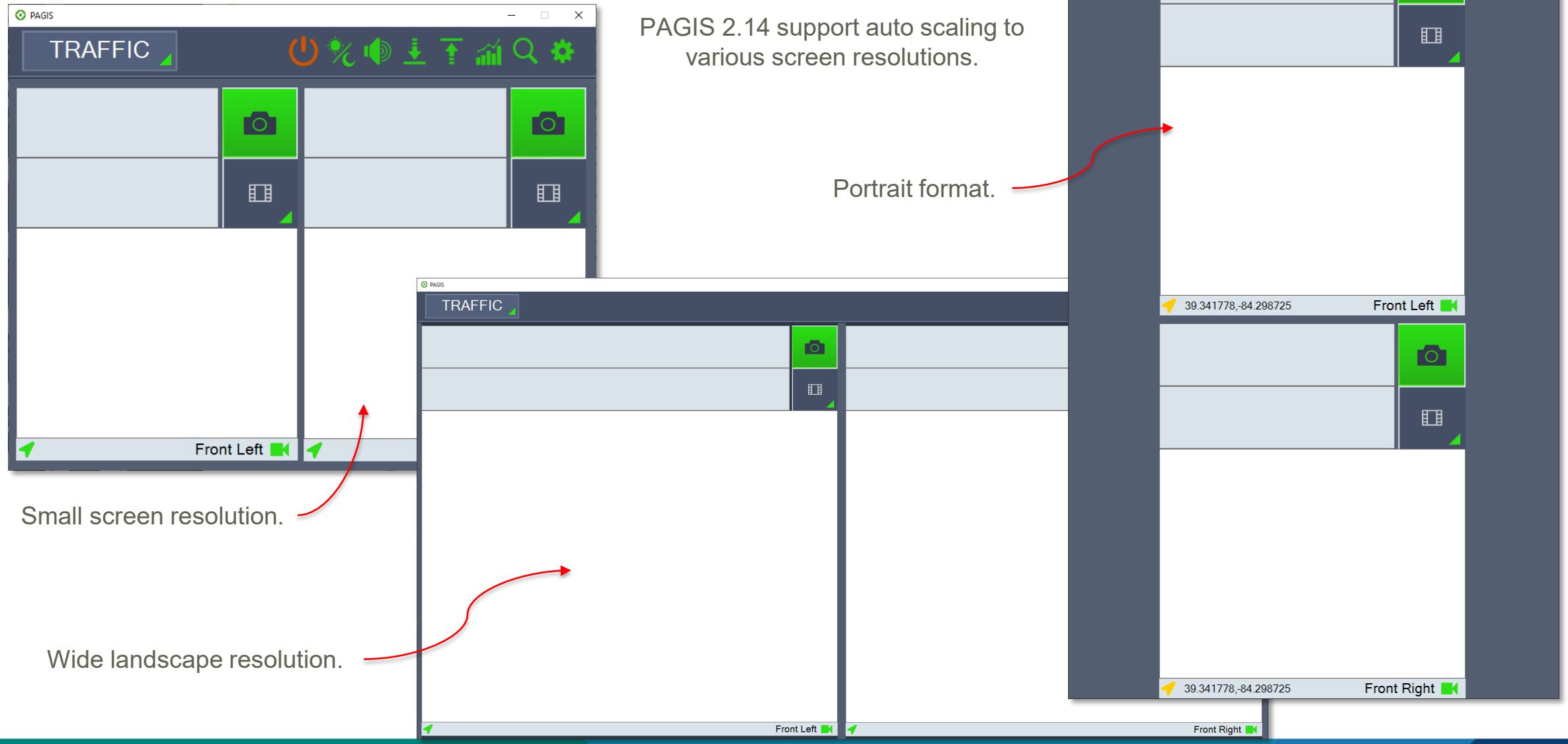
GPS Coordinates

Camera Title

Copyright © 2021 Neology, All Rights Reserved.

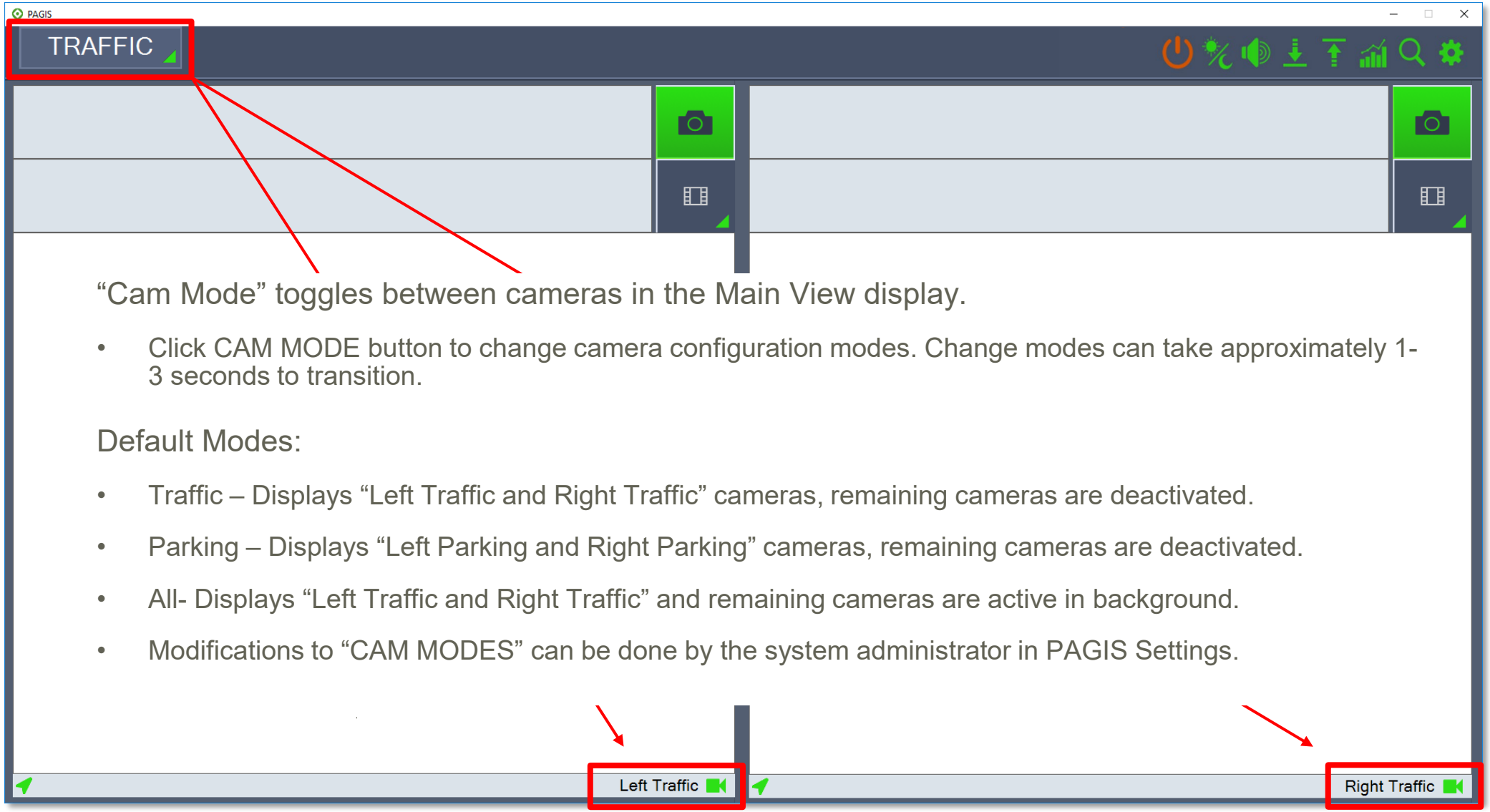
Auto Screen Scaling

PAGIS 2.14 support auto scaling to various screen resolutions.



Copyright © 2021 Neology, All Rights Reserved.

Camera Mode



"Cam Mode" toggles between cameras in the Main View display.

- Click CAM MODE button to change camera configuration modes. Change modes can take approximately 1-3 seconds to transition.

Default Modes:

- Traffic – Displays "Left Traffic and Right Traffic" cameras, remaining cameras are deactivated.
- Parking – Displays "Left Parking and Right Parking" cameras, remaining cameras are deactivated.
- All- Displays "Left Traffic and Right Traffic" and remaining cameras are active in background.
- Modifications to "CAM MODES" can be done by the system administrator in PAGIS Settings.

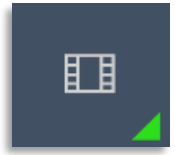
Copyright © 2021 Neology, All Rights Reserved.

Camera Controls

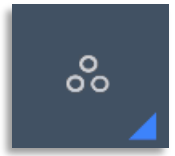




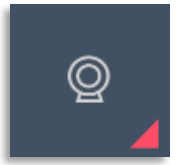
Take Pic: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.



Static View: This is the default state at login showing the Static View of captured events.
(NOTE: PAGIS does not automatically display a live feed.)



Color View: Clicking the Camera View selector button once, will switch to the Color View Mode. This displays the current live view of the color camera and will time out after 60 seconds or until the next capture event, which ever occurs first.



IR View: Clicking the Camera View Selector button twice, will switch to the Infrared (IR) View Mode. This displays the current live view of the IR camera and will time out after 60 seconds or until the next capture event, which ever occurs first.

Copyright © 2021 Neology, All Rights Reserved.

Take Picture

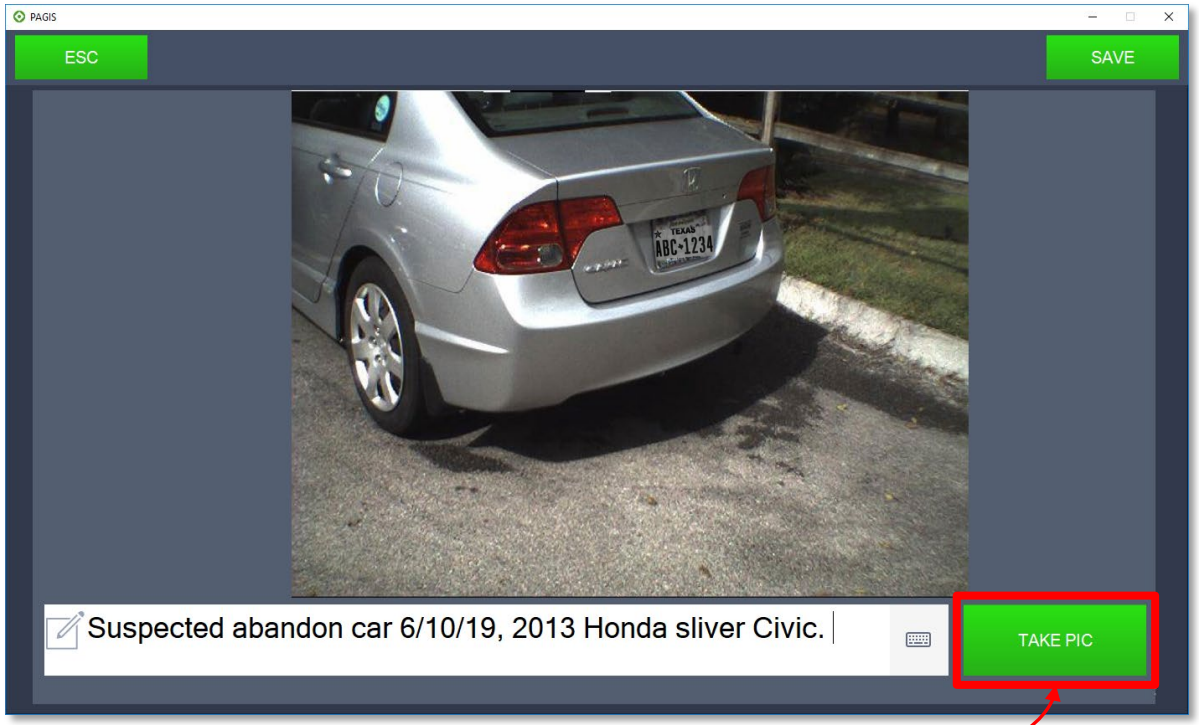
Take a Picture:

- From the Main View Screen, press the Take Pic button from the desired camera.
- The image taken will be displayed.
- Enter a description of the picture in the text field at the bottom of the screen.
- To save picture click the SAVE button, ESC to cancel. Either action will return you to Main View Screen.

NOTE: The picture will not be saved if a description note is not entered in the text box.

View the Saved Images:

- Navigate to the Review menu in PAGIS.
- Select Audits.
- The user will be able to see a thumbnail of the image and the saved text/note.
- In order to review the saved images beyond a shift, the user will need to run the Audit Image Report from BOSS.



Toggle “Take Pic” button to activate live and capture mode.

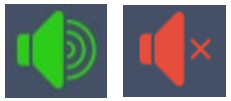
Copyright © 2021 Neology, All Rights Reserved.

System Controls





Logoff button: Located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen. When Auto-login is enabled this will close PAGIS.



Sound button: When selected, this button with toggle the PAGIS Read capture sound On or Off, alert sounds will remain activated.



Day/Nite mode: Switch PAGIS between day & night mode screen skins.



Begin Shift / Download button: When activated, this begins downloading assigned data from the BOSS server.



End Shift / Upload button: When selected, this will upload any previously unsent Reads/Hits, images, and Audits to the BOSS server.



Statistics/Review button: When selected the user can review Alert list, Reads, Hits, Targets, and other PAGIS information.



Search button: When selected the user can research all available Reads/Hits as well as manually add a license plate to PAGIS's local alert list "Manual Reports".



Settings button: This button is only viewable to Admin level users and allows for system configuration changes and setup.



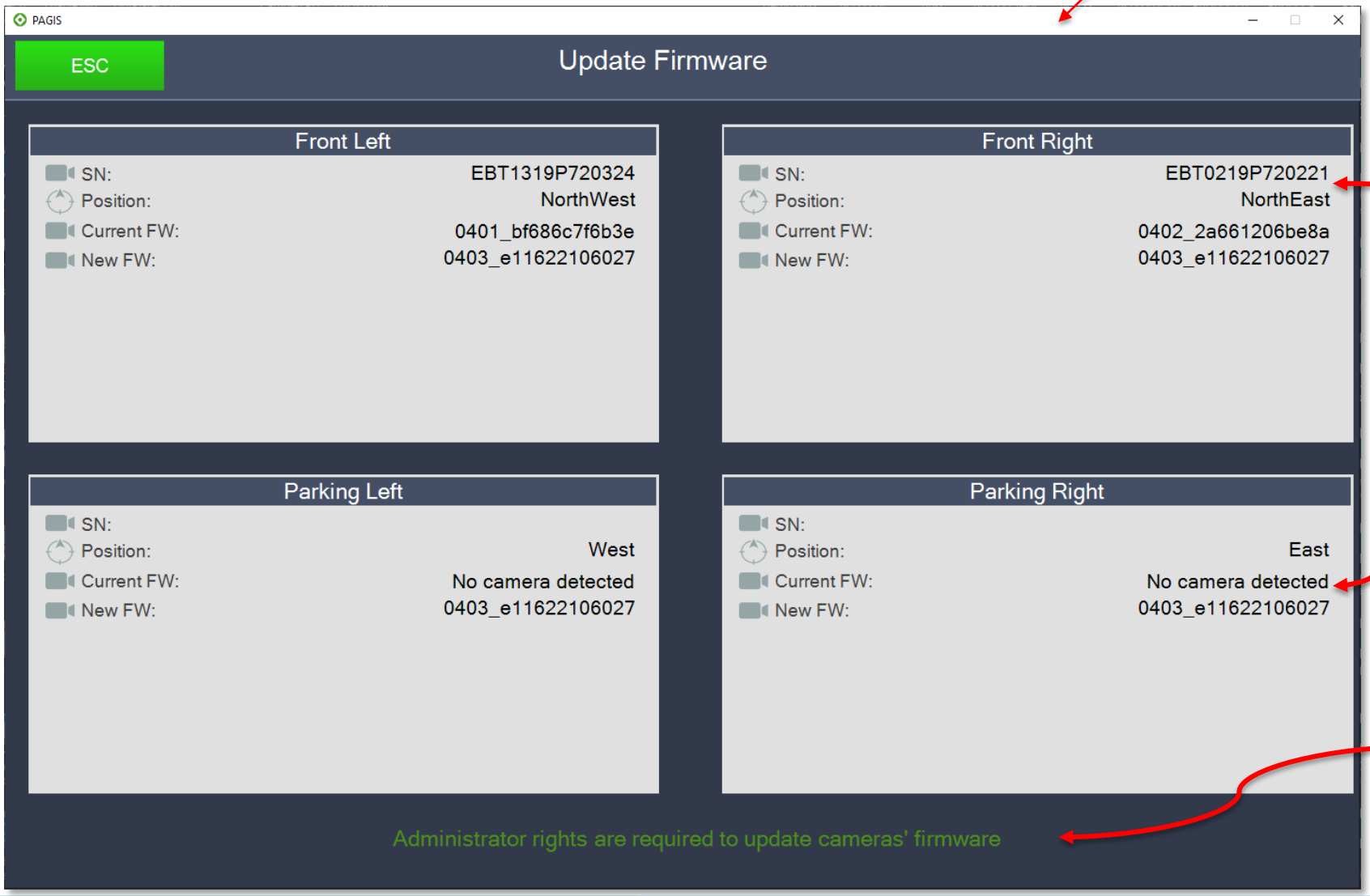
Firmware update: This icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

Copyright © 2021 Neology, All Rights Reserved.

Camera Firmware Update

(Restricted Users)





Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance.

Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version,
- New FW version available.

The firmware update process only updates camera that are attached and function on the mobile processor.

Restricted PAGIS users are only notified and displayed update information. Administrator must log into PAGIS and apply the FW update.

Copyright © 2021 Neology, All Rights Reserved.

Night Mode Screens

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



Copyright © 2021 Neology, All Rights Reserved.

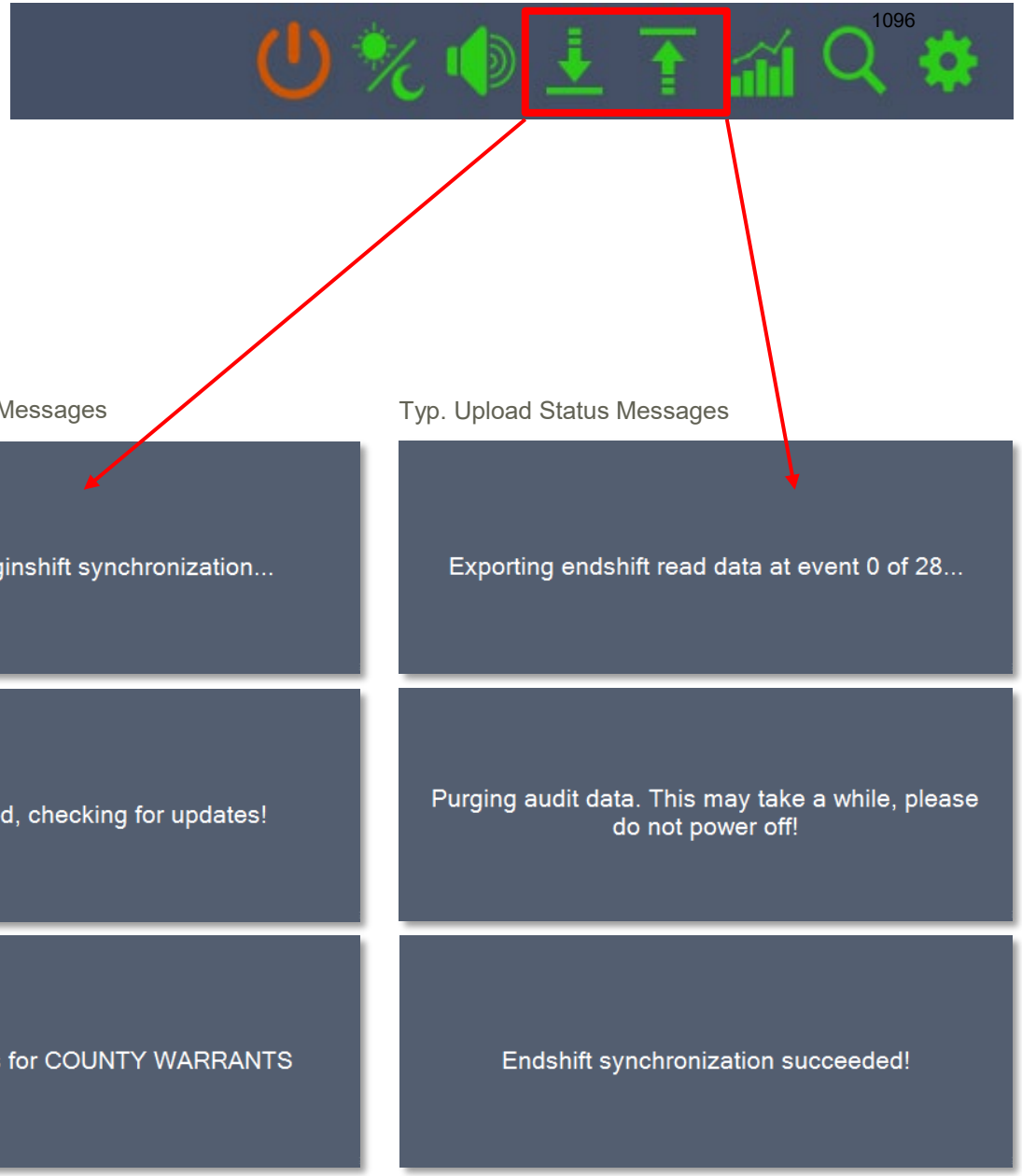
Data Synchronization

Data synchronization can be configured one of three ways depending on usage type. Its important to understand which option PAGIS is configured for as they dictate different user interaction.

USB Sync- This method of synchronization requires that the PAGIS user manually activate the upload/download button to send/retrieve data from external USB drive.

Boss Sync without Purge- When “Boss-Sync” is enabled all data will be automatically synchronization between PAGIS and BOSS, this included Users, Alert-List, Reads/Hits & Audit data. The exception in this option is that locally stored data remains accessible in PAGIS, this includes Reads/Hits & Manual Reports entries. Reads/Hits & Manual Reports will remain local until the Upload button is activated upon which those data sets will be purged from PAGIS.

Boss Sync with Purge- When “Boss-Sync” is enabled all data will be automatically synchronization between PAGIS and BOSS, this included Users, Alert-List, Reads/Hits and Audit data. With the Purge setting enabled it is not necessary for the PAGIS user to manually activate the Upload button to purge locally stored data as this will be maintained by PAGIS based on Purge settings configured, purging occurs each time PAGIS is launched.



Copyright © 2021 Neology, All Rights Reserved.

First Time PAGIS Activation

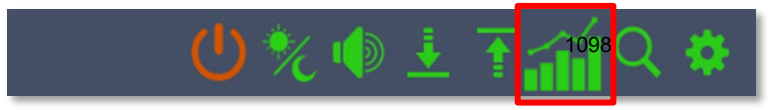


Unlike the fixed cameras the mobile system only needs to communicate with BOSS3 or BOSS4 to register its existence, plate data packet not required.

- PAGIS auto sync cycle can accomplish this automatically once the primary BOSS IP has been entered and saved, typically auto sync will occur around 10-20 seconds after setting was applied. Sync status messages are not displayed on-screen during an auto sync event.
- Activating the download button will manually initiate communication with BOSS, during this process the user will see sync status messages. First time synchronization BOSS will acknowledge the communication with a rejection message titled “HttpStatusCode Unauthorized” signifying BOSS has seen the request, created the device listing but rejects the communicated pending user activation in BOSS.

Copyright © 2021 Neology, All Rights Reserved.

Review



Click Review from the Main View screen to display additional options for reviewing data.

- **Total Reads-** Shows the total number of Reads/Hits collected and the amount synced.
- **Reads-** Shows only the total number of collected Reads.
- **Hits-** Shows only the total number of collected Hits.
- **Misreads-** Shows only the total number of Reads marked as misreads.
- **Audits-** Shows the total number of collected Audits and the number that have synced with BOSS.
- **Targets-** Shows only the number of targets downloaded, they do not sync as they originated from the Boss application.

Note: When PAGIS is setup for Disk-Sync the “Sync” column dose not apply.

Reads- Review all plate detections that have occurred since the last upload or data purge cycle.

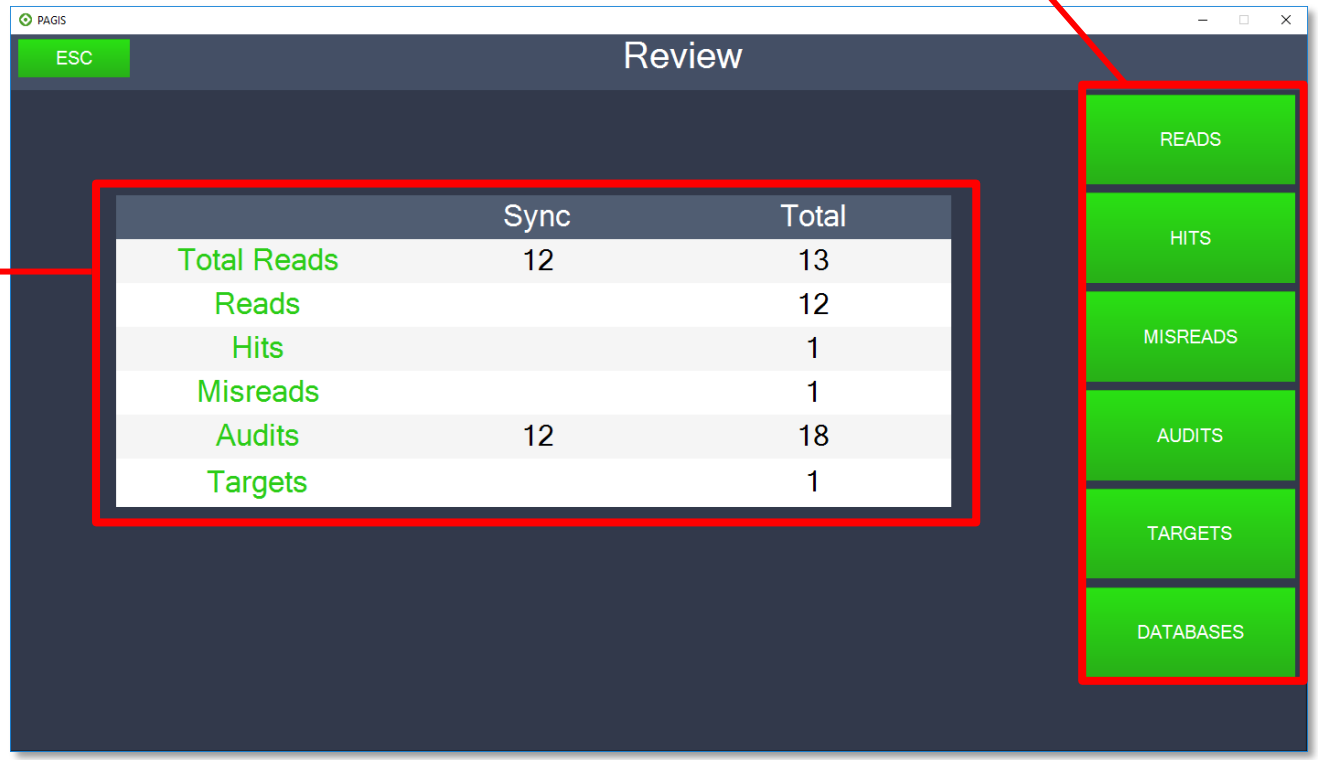
Hits- Review Hit alerts that occurred since the last upload or data purge cycle.

Misreads- Review Reads that have been manually flagged during the shift as misreads.

Audits- Review failed and successful login’s, any manual data entered during the shift, pictures taken and all manual license plate searches.

Targets- Review targets that have been synchronized from Boss.

Databases- Review the all the databases currently in PAGIS.



Copyright © 2021 Neology, All Rights Reserved.

Review- Reads

Save changes or Esc to return to Main View.
(Typ. thought out review screens)

Current view / Total Reads.
Prev. & Next

Options not available in
Reads review screen.

IR “Plate Patch”
Clicking Plate Patch will result in larger view
Of image for 4sec.

OCR translation of “Plate Patch”
Click OCR Patch to correct a misread.

- Address based on GPS
- GPS
- Time/Date
- Camera Name

Color Camera “Overview” image
Clicking Overview Patch will result in larger view
Of image for 4sec.



Active Map w/
map controls

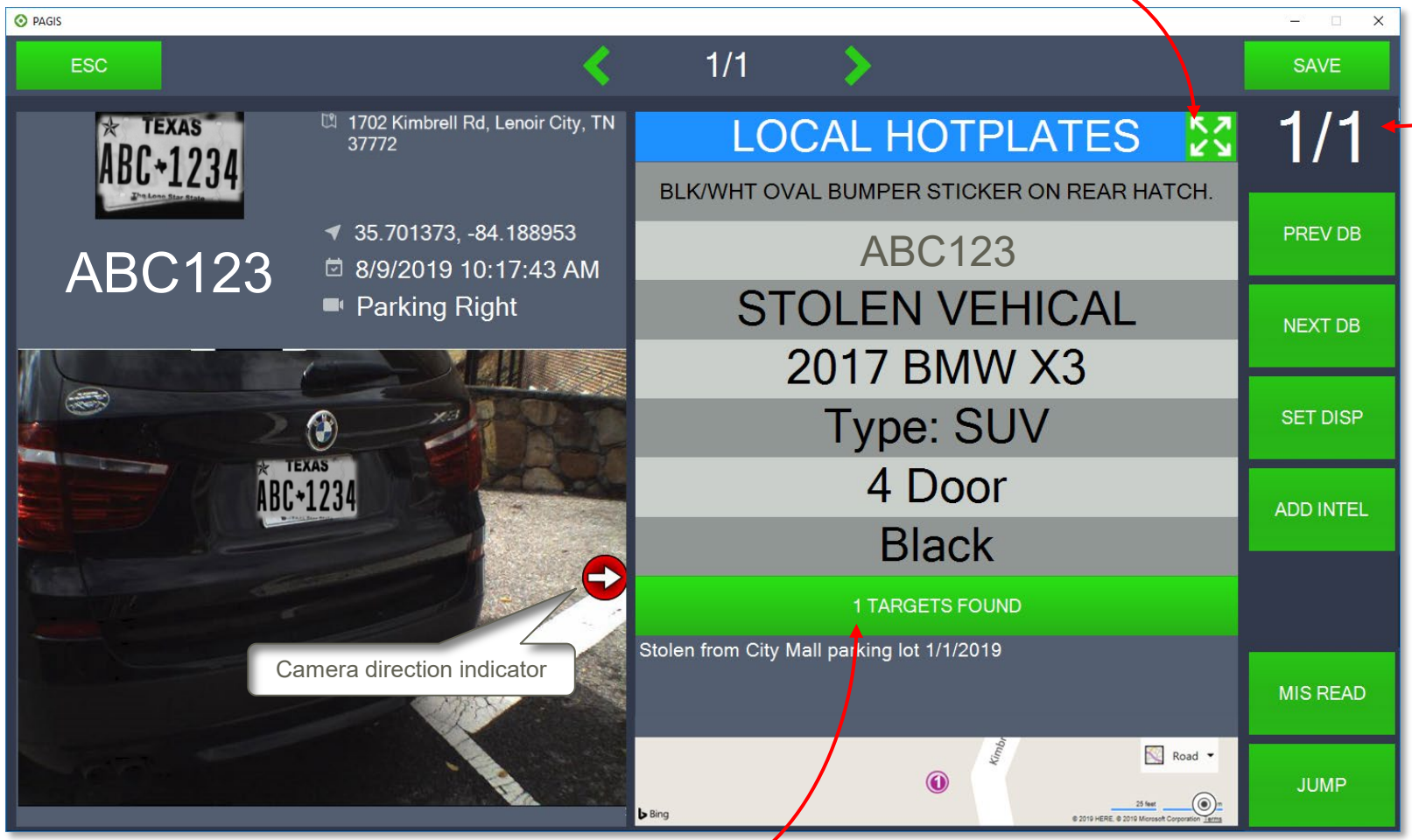
Jump –Move to a specific record.

Copyright © 2021 Neology, All Rights Reserved.

Review- Hits

Current/Total (Databases) – Shows how many Alert List the Hit has registered against. For example, 1/3 means that you are viewing information from the first of the three databases that produced Hits on this plate capture.

Expand full Map

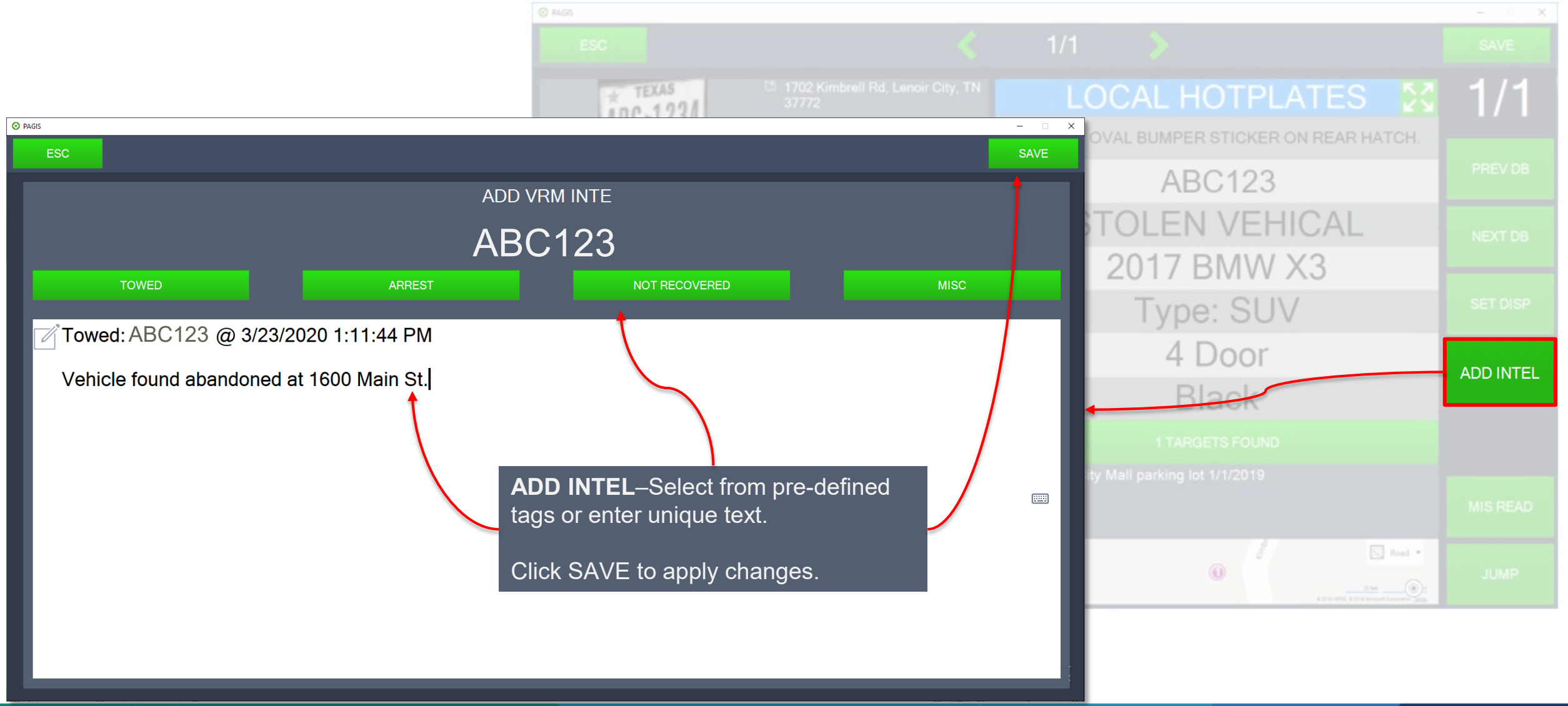


Target Profile Found
Click to view

- **Prev DB** – Moves to the previous Alert List that produced a Hit alert with current plate number.
- **Next DB** – Moves to the next Alert List that produced a Hit alert with current plate number.
- **Set Disp** –Report the disposition of a Hit in one of the categories defined by your Boss system administrator, *(Arrest Made, Vehicle Recovered, Surveillance Established, Towed, etc.)*. Dispositions appear in sperate selection window, these dispositions are reported to BOSS and allow for more detailed classification when running a Hit reports.
- **Add Intel** – Add information about a particular Hit prior to synchronization to BOSS. For instance, you might add information about the arrest or violation.

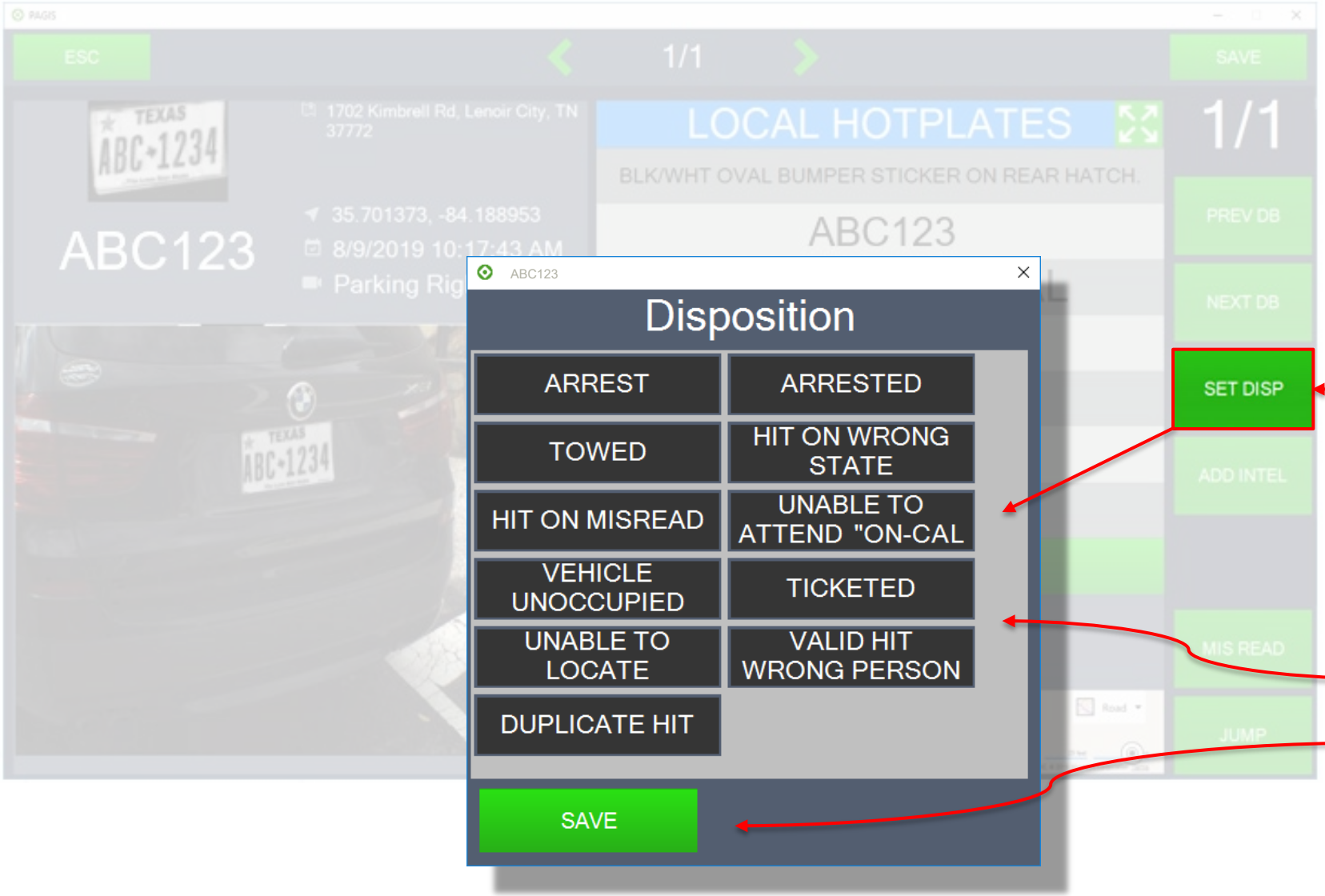
Copyright © 2021 Neology, All Rights Reserved.

Review- Hits- Add Intel



Copyright © 2021 Neology, All Rights Reserved.

Review- Hits- Disposition



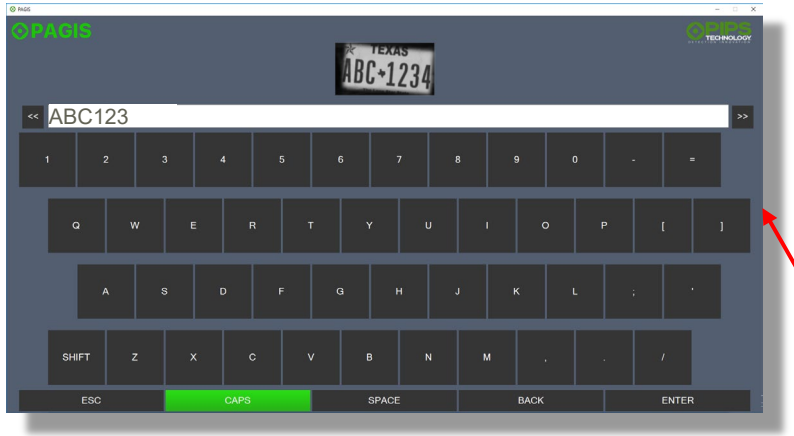
Set Disp –Report on the disposition of the Hit from the deployed categories.
Note: Dispositions are managed by BOSS, additions or edits must be done by system admins.

Select one or multiple.

Save to apply.

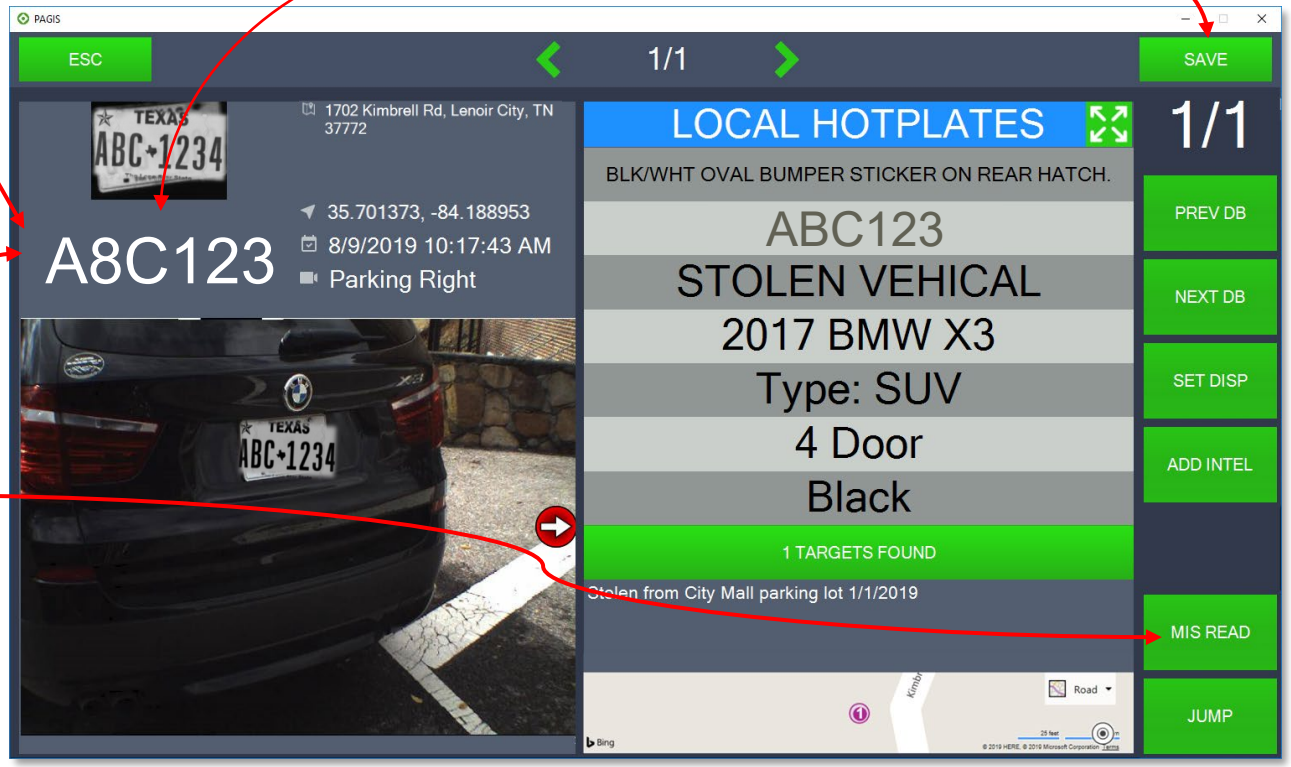
Copyright © 2021 Neology, All Rights Reserved.

Misread Correction



Misread Hit.

Save changes



Correct or tag Read/Hit that have been misread.

- *Click OCR Patch to manually correct a misread, "ENTER" to save.*
- *Click* MISREADS *button to instantly tag event as "Misread" without editing "SAVE" to apply.*
- *Hits tagged as misread are demoted to Read and no longer counted as Hit.*

Copyright © 2021 Neology, All Rights Reserved.

Review- Targets

TARGET 1104 S

Clicking Prev & Next will cycle through all available Targets.

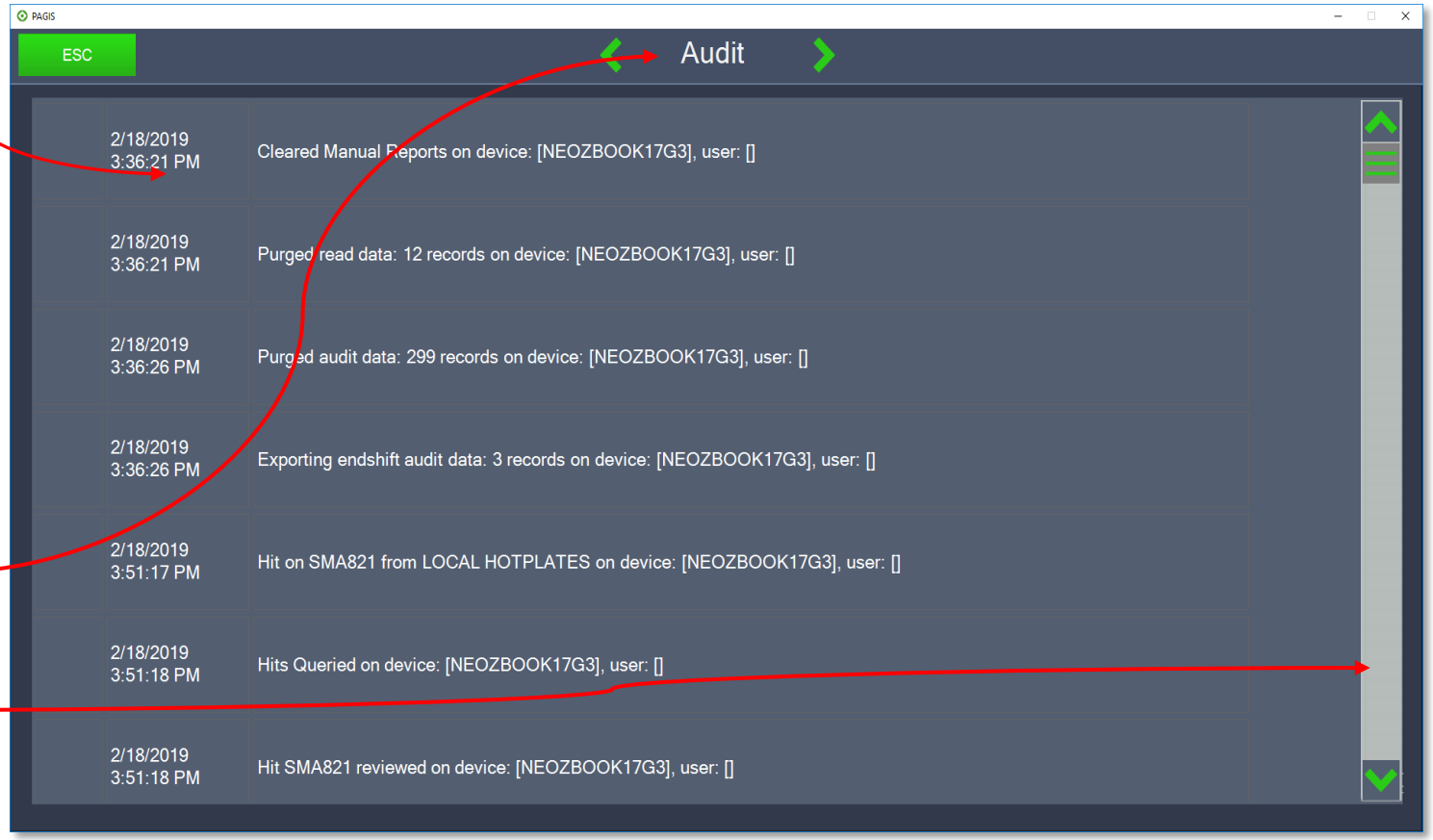
- **Target Profile**–Target screen displays information about suspects matched with a license plates. Targets are downloaded into PAGIS Targets list from the Back Office System Software (BOSS).
- Targets review also available through associated Hits, see example on Slide 11.
- **Jump**- Move to a specific record
- **Close** – Returns to previous screen.



Copyright © 2021 Neology, All Rights Reserved.

Review- Audits

- The Audits screen provides a log of various actions taken during the current session, including searches, synchronizations, Hits, etc. Audit trail is reset during Upload or Auto purge cycle.
- Audit logs are transmitted back to BOSS during Auto-Sync or during a manual Upload cycles.
- **Esc-** Return to previous screen.
- **Prev / Next-** Cycle thought all available audit log by page.
- **Scroll-** Scroll thought all available Audits.



Copyright © 2021 Neology, All Rights Reserved.

Review- Databases

Database Name – Displays the name and color code of the Alert List, along with Date\Time showing the last synchronization update.

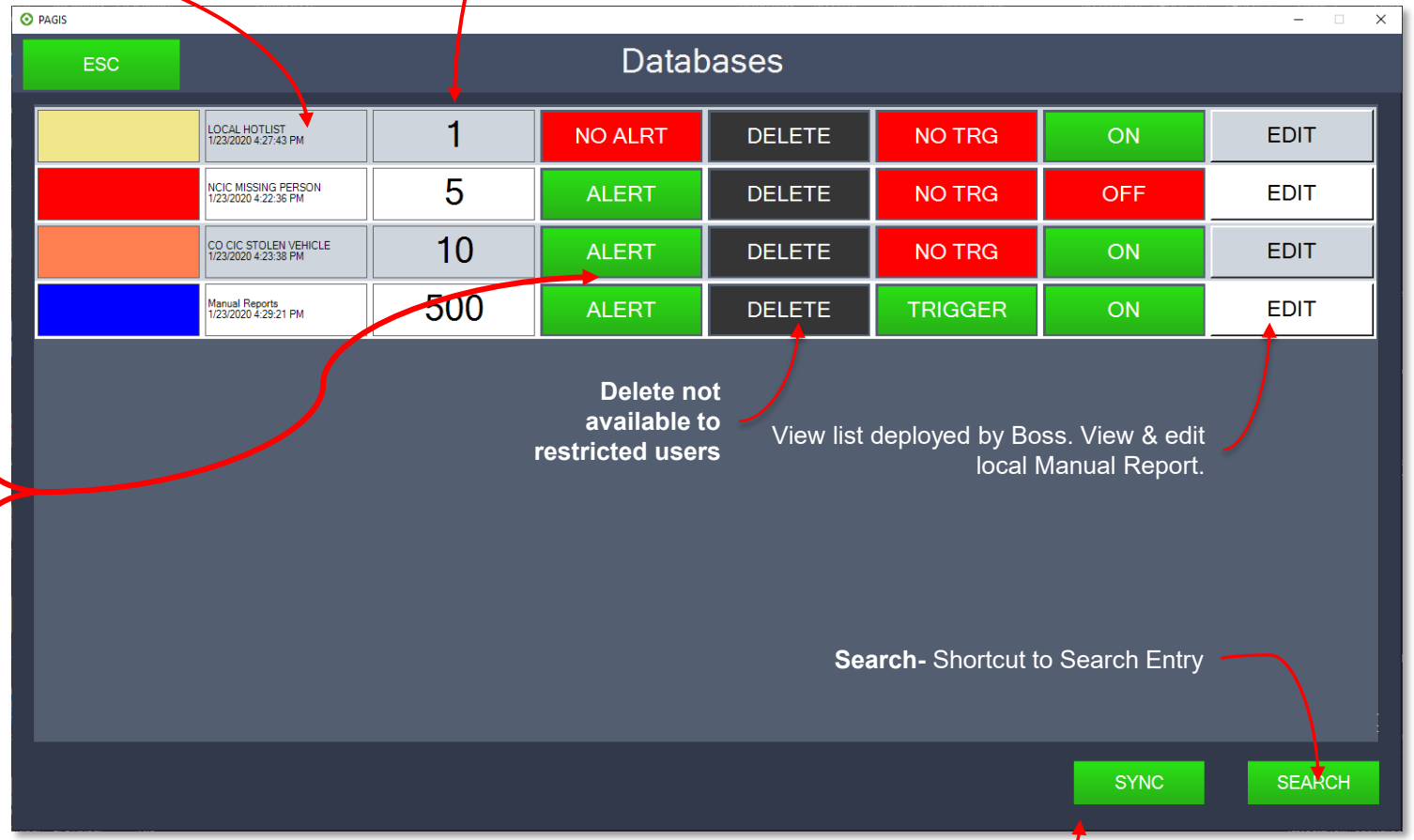
Alert/No Alert - When this button is clicked it will switch from “Alert” or to “No Alert” depending on its previous state. “Alert” means the PAGIS user will be alerted if a Hit occurs. If “No Alert” is displayed the PAGIS user will not be notified of alert, but the alert will still register.

Delete – Removes the Alert List from the current session. Because some databases may be managed in BOSS, if deleted and has not been removed from the BOSS deployment list, it will be added back on the next synchronization via Auto-Sync or during the next Download cycle.

Trigger/No TRG – If Trigger is on, the software sends a signal to a com port on the mobile processor and any device (such as a light or siren) connected through this port will active the device during an alert.

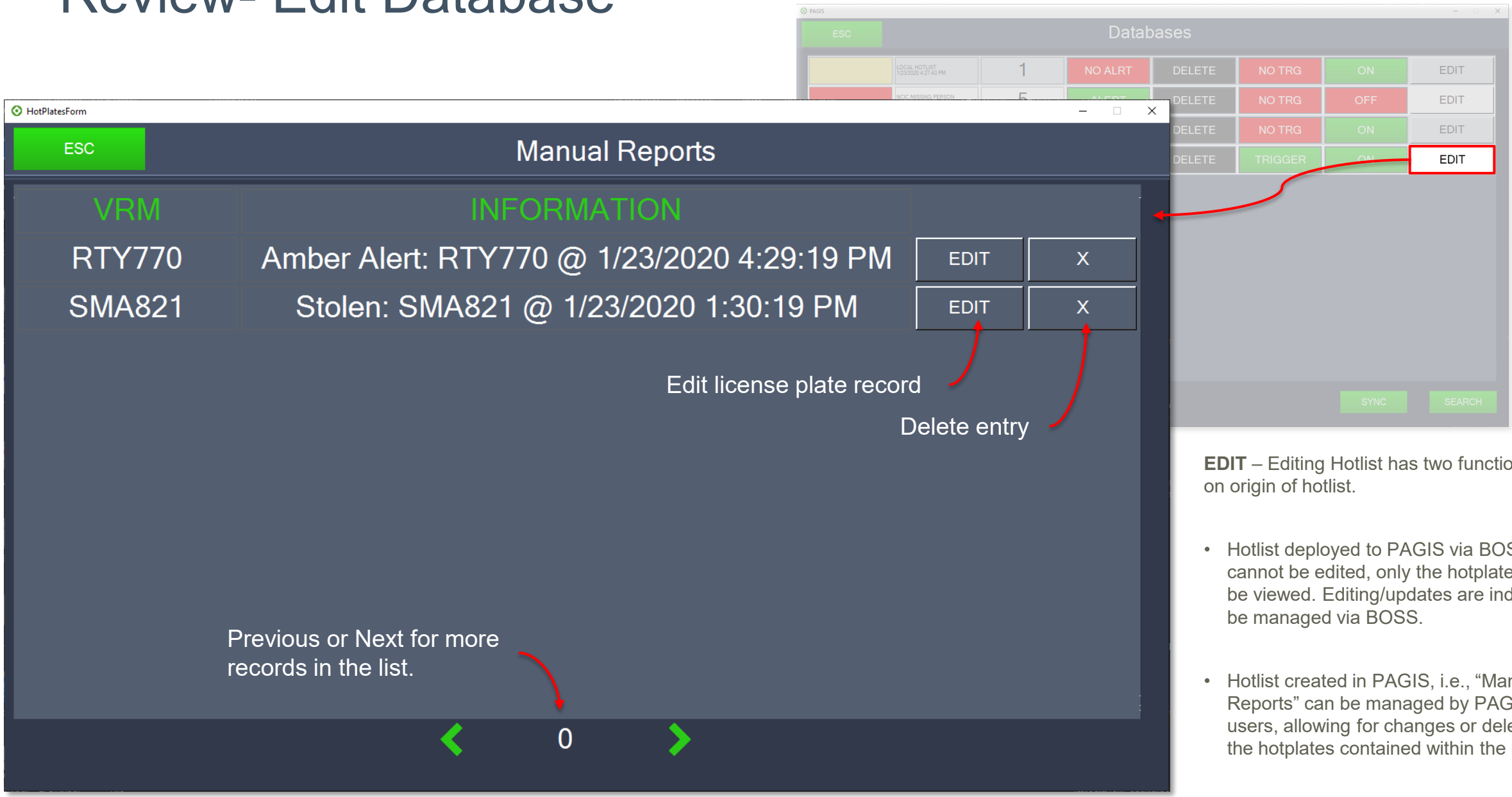
On/Off – Database status indicator. A green On button indicates that the Alert List is active. A red Off button shows that the Alert List is inactive, and Hits will not be generated from that Alert List in PAGIS.

Priority – Database priority provides PAGIS a means of displaying Hits with higher priority first if multiple Hits occurs from a single event. Values can be (1-999) as determined by BOSS System Administrator. The lower the number, the higher the Alert List priority. By default, the “Manual Reports” Alert List created by PAGIS has a priority of 500.



Copyright © 2021 Neology, All Rights Reserved.

Review- Edit Database



EDIT – Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e., “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.

Copyright © 2021 Neology, All Rights Reserved.

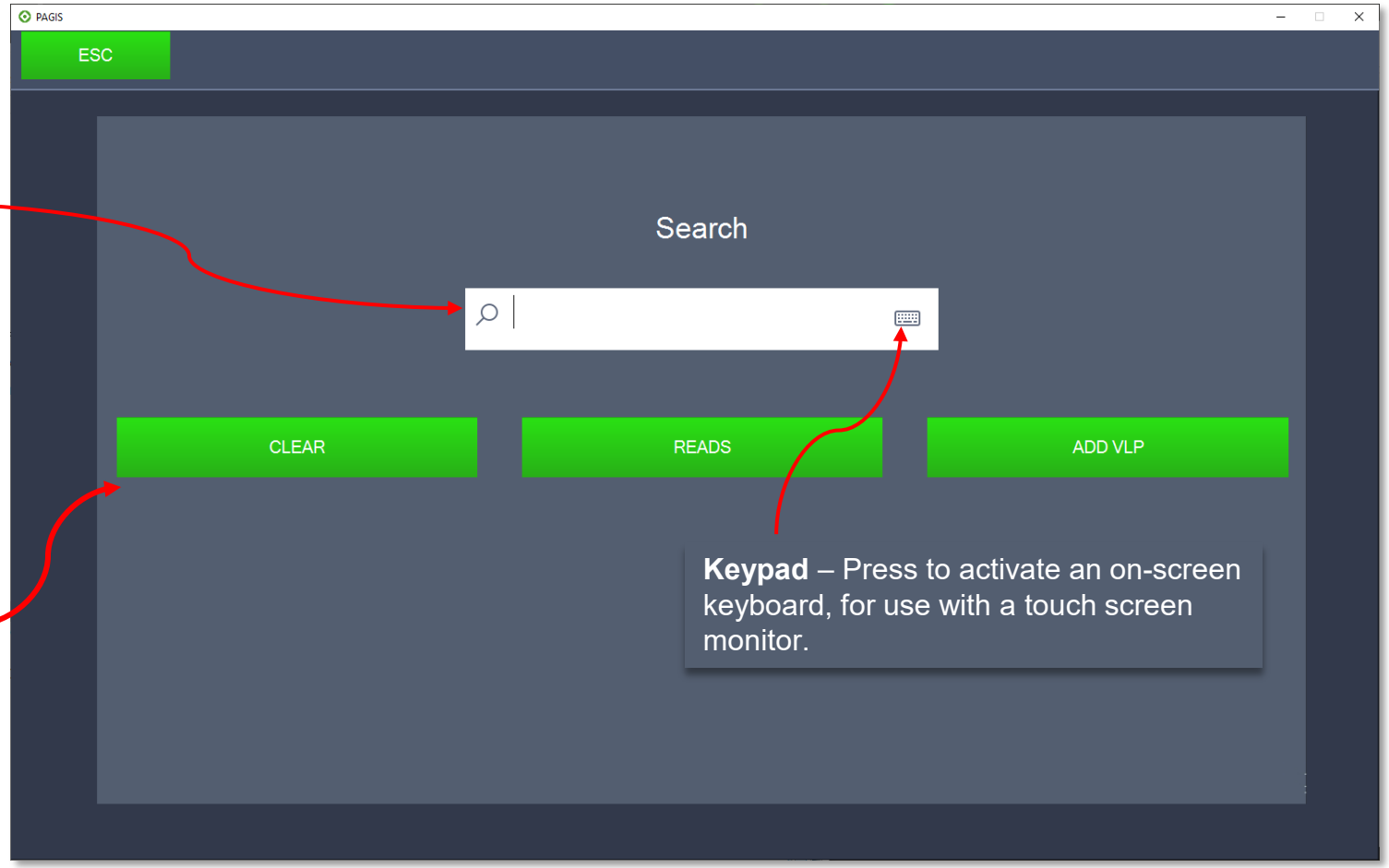
Search Entry



Search Entry button.

Click Search Entry from the Main View screen to display Search features.

- **Text Field** – Enter the alphanumeric string to search. Accepted wildcards are Asterisk “*” or Underscore “_”.
- **Clear** – Clear the content of the text box.
- **Reads** – Search for plate number with the Reads and Hits currently stored in the PAGIS.
- **Add VLP** – Add plate to “Manual Reports” Alert List or check existing databases for the entered license plate. Partial plates or wildcards not accepted.
- **Esc** – Return to the previous screen.



Copyright © 2021 Neology, All Rights Reserved.

Search Entry- Reads

READS Searching against collected license plate data in PAGIS.

- Search criteria can include exact text or text and wildcards. Wildcards are special characters that represent any / all potential characters and can be used in searches and queries.

- Wildcard searches can be performed using the * and _ characters. The asterisk (*) designates an unknown number of characters while the underscore (_) indicates a single missing or unknown character. To search for a plate number with the characters 3 and C, entering *3_C* will display all records containing 3 and C separated by one character.



Copyright © 2021 Neology, All Rights Reserved.

Search Entry- Reads

Current / Total Reads.
Prev. & Next

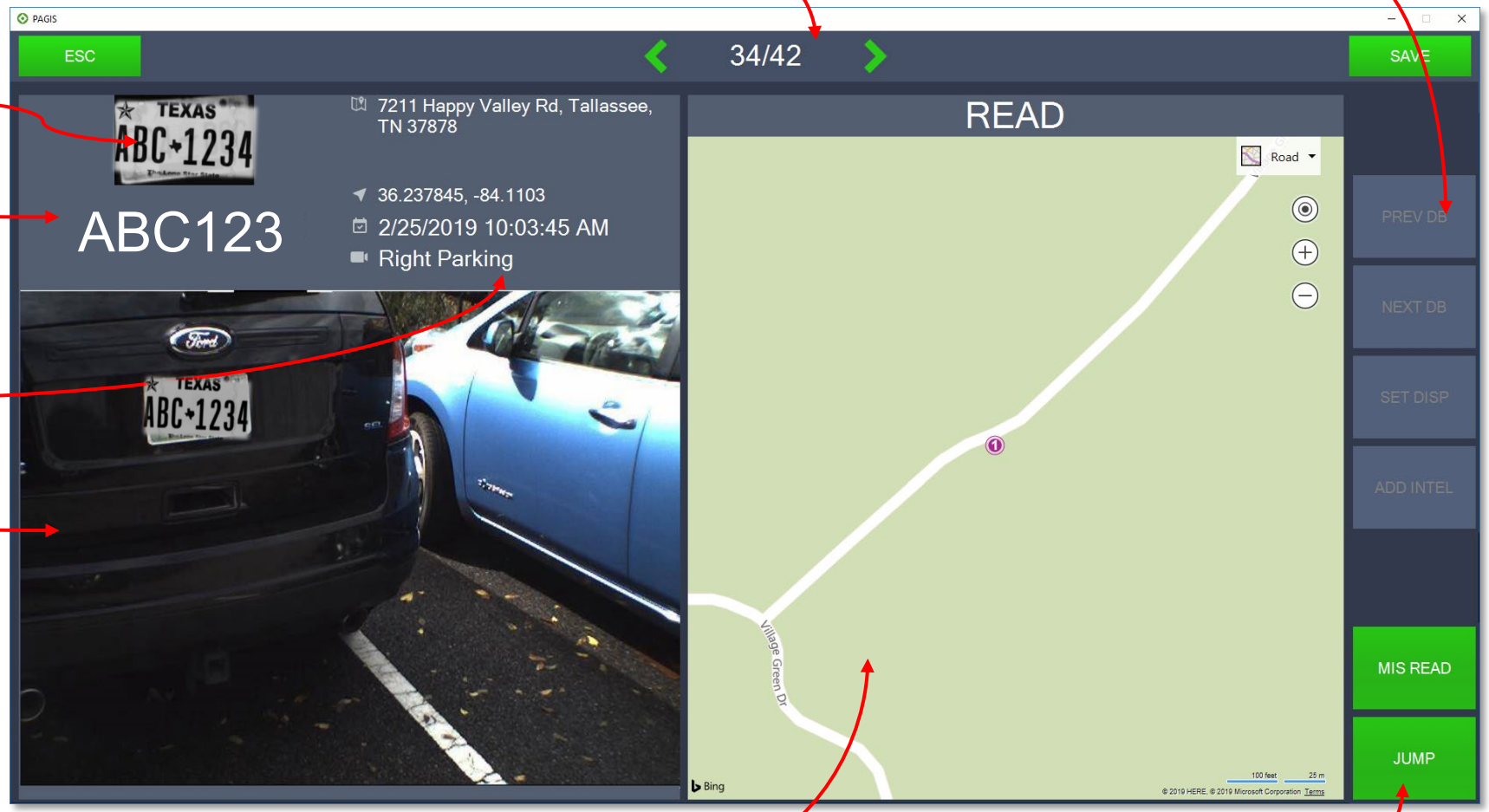
Options not available in Read review screen.

IR “Plate Patch”
Clicking Plate Patch will result in larger view Of image for 4sec.

OCR translation of “Plate Patch”
Click OCR Patch to correct a misread.

- Capture Address
- GPS
- Time/Date
- Camera Name

Color Camera “Overview” image
Clicking Overview Patch will result in larger view Of image for 4sec.



Active Map

Jump –Move to a specific record.

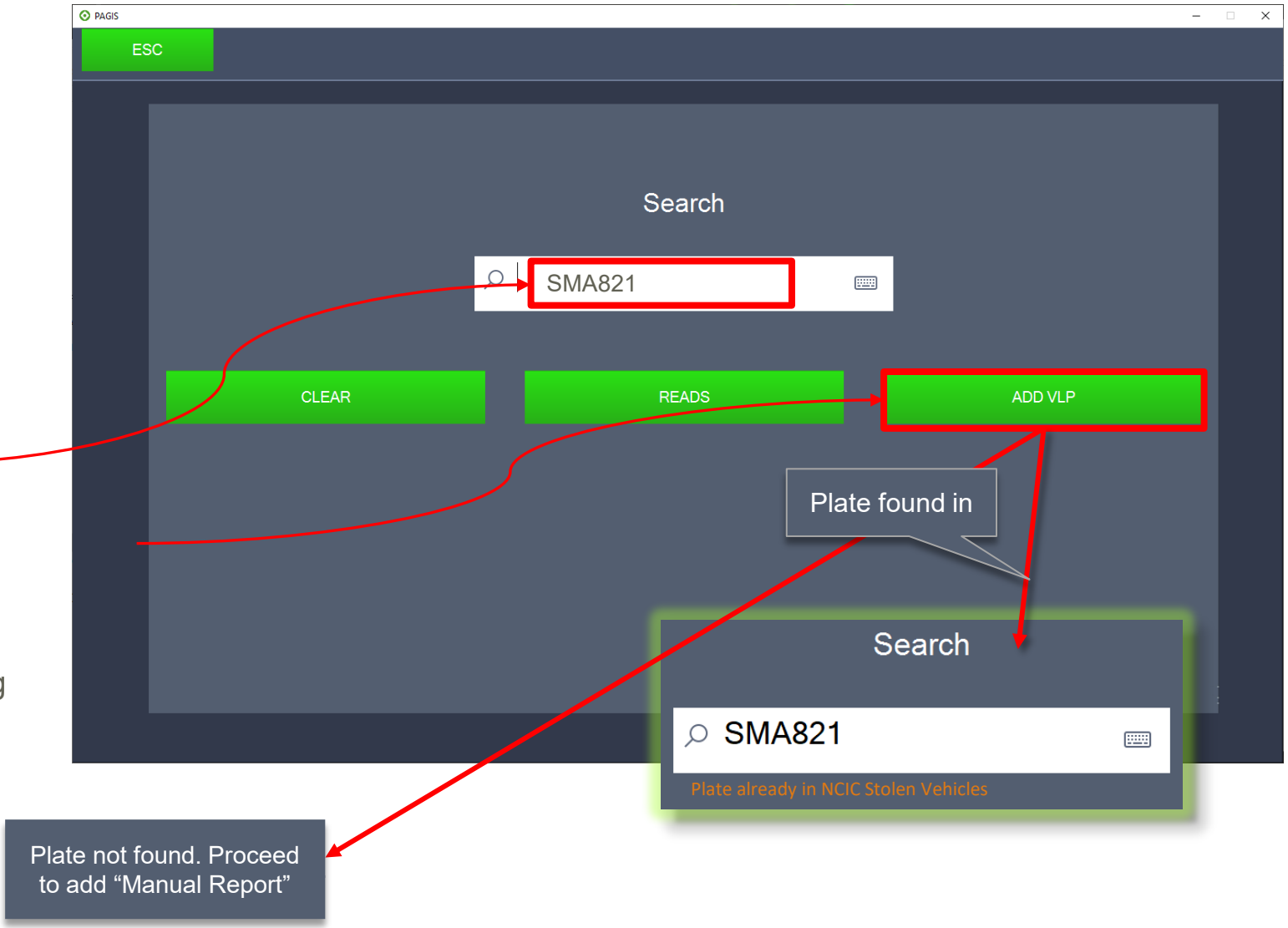
Copyright © 2021 Neology, All Rights Reserved.

Search Entry- ADD VLP

ADD VLP

Add a plate to “Manual Reports” Alert List or check for existence of plate in Alert List download from Boss.

- Manual Reports is PAGIS standalone Alert List designed for manual entries by the PAGIS operator.
- Manual Reports Alert List do not transfer to Boss or other mobile units utilizing PAGIS.
- Manual Reports Alert List are cleared out during a manual “upload” or Purge cycle.
- Enter plate into the text field, click “Add VLP”.
- If plate already exist, a message will applier indicating the Alert List it was found in. Otherwise, you will be prompted in the next screen to classify your entry.
- Wildcards or partial plates not accepted when adding VLP’s.

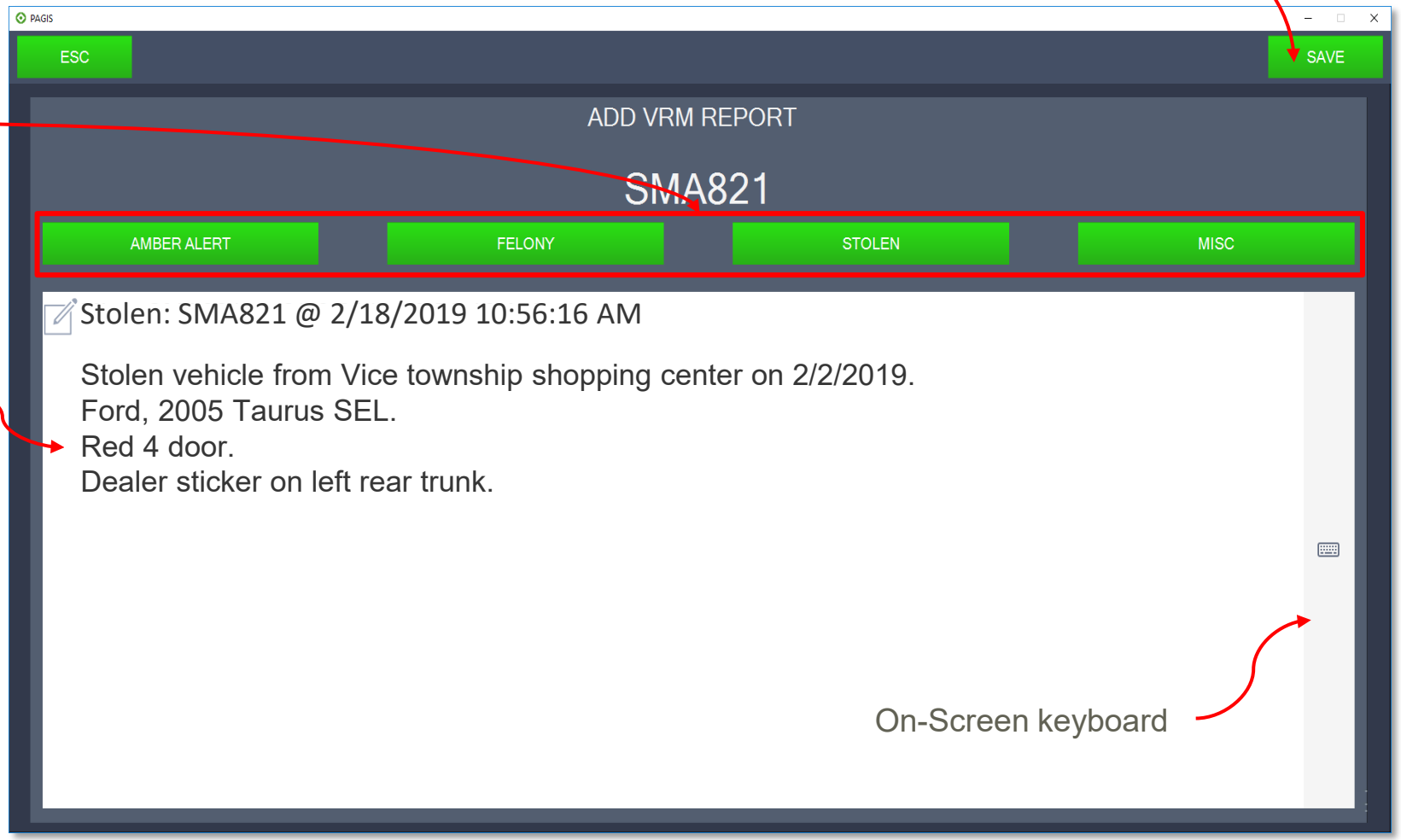


Copyright © 2021 Neology, All Rights Reserved.

Search Entry- ADD VLP

ADD VLP Report:

- Select one of the four pre-defined classifications.
- Type in additional information about the vehicle.
- There is no limit to the number of manual entries that can be added to the Manual Report Alert List.
- Entries can be edited or deleted individually in the review Database section.
- All entries in the Manual Report Alert List will be discarded when a manual End Shift is performed.



Copyright © 2021 Neology, All Rights Reserved.

End of PAGIS User Training



Thank you

Copyright © 2021 Neology, All Rights Reserved.



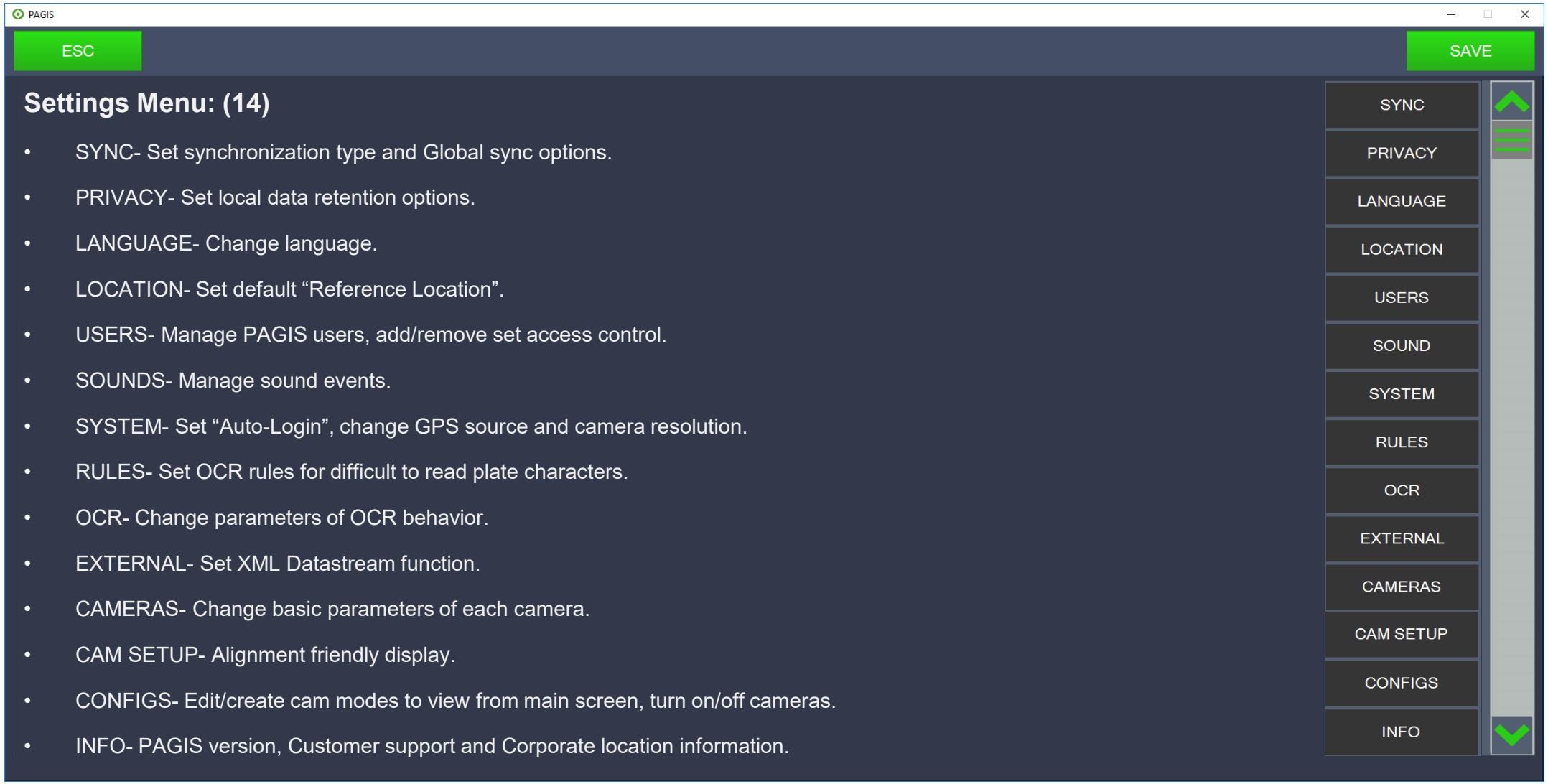
Administration Training

PAGIS Settings

Settings- Section Definitions



Setting button from Main View screen.



- SYNC- Set synchronization type and Global sync options.
- PRIVACY- Set local data retention options.
- LANGUAGE- Change language.
- LOCATION- Set default “Reference Location”.
- USERS- Manage PAGIS users, add/remove set access control.
- SOUNDS- Manage sound events.
- SYSTEM- Set “Auto-Login”, change GPS source and camera resolution.
- RULES- Set OCR rules for difficult to read plate characters.
- OCR- Change parameters of OCR behavior.
- EXTERNAL- Set XML Datastream function.
- CAMERAS- Change basic parameters of each camera.
- CAM SETUP- Alignment friendly display.
- CONFIGS- Edit/create cam modes to view from main screen, turn on/off cameras.
- INFO- PAGIS version, Customer support and Corporate location information.

Copyright © 2021 Neology, All Rights Reserved.

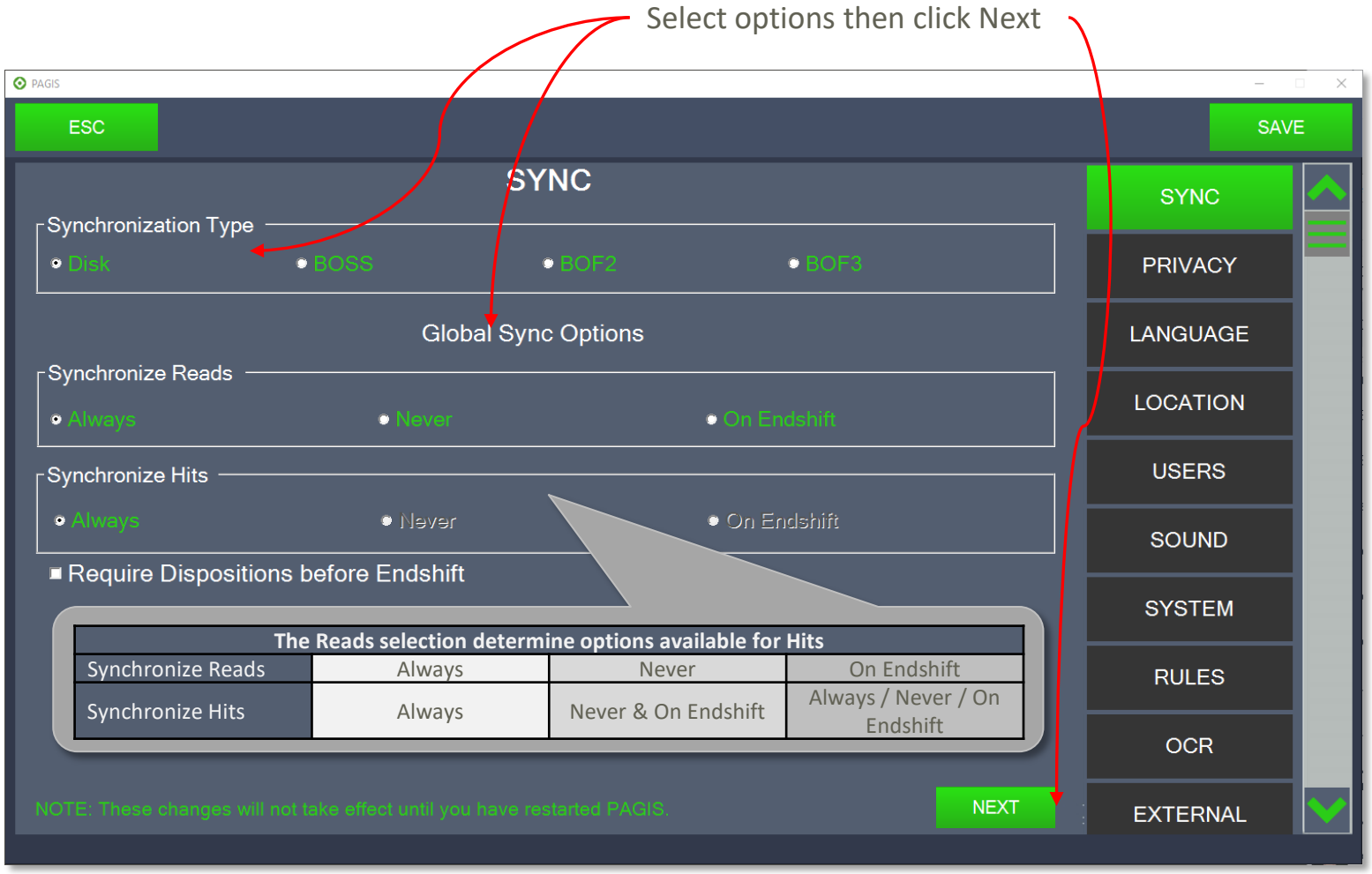
Synchronization

PAGIS Sync Type:

- **Boss-** Configure PAGIS communication to BOSS via TCP/IP. Once established communication to Boss can occur automatically or manually via the Upload/Download features.
- **Disk-** Configure synchronization via USB thumb drive.
- **BOF2,3-** Used for European Boss version (Instation).
- **Next-** Proceeds to next configuration screen based on option selected above.

Global Sync Options: (Synchronize Reads / Hits)

- Selecting "**Always**" means that Reads and Hits are always going to be synced to the Back Office System Software.
- Selecting "**On Endshift**" means that syncing will only occur upon Upload or Sync.
- Selecting "**Never"** means that information gathered in the PAGIS Software will be "Sanitized" during a manual Upload operation, Data WILL NOT be sent to its destination.
- Checking the "Require Dispositions before Endshift" box will require the user to select a disposition for each of the Hits that has occurred before a manual Upload can complete.



Copyright © 2021 Neology, All Rights Reserved.

Sync-Disk

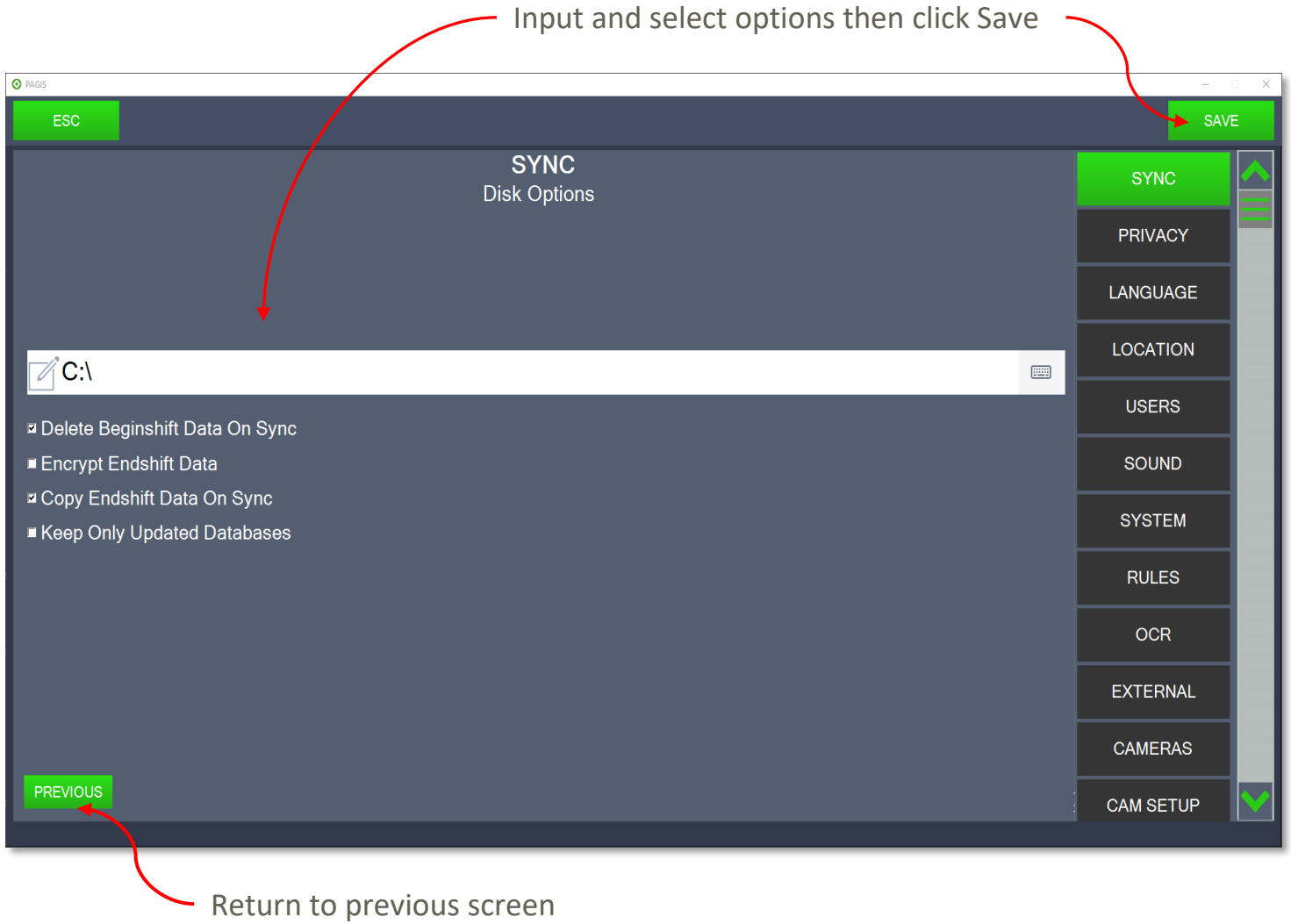
Synchronization to Disk:

If choosing Disk, with the sync folders residing on a USB flash drive, make sure the flash drive assigned to the user has adequate space to accommodate the file size of all the databases that will be imported and exported. Folder sizes vary depending upon the number of entries and the number of databases but typically a 4Gb drive will work for most.

- **Text Field-** Enter the drive letter only, do not use folder paths as PAGIS will automatically manage Begin Shift and End Shift folders creation and deletion.

Disk Sync Options:

- **Delete Begin Shift data on sync-** If this option is selected, the sync folder will be deleted once all of the data has been imported into the PAGIS Software. This option is “on” by default.
- **Encrypt End Shift data-** If this option is selected, the End Shift files created by PAGIS will be encrypted. This option is “off” by default.
- **Copy End Shift data on sync-** If this option is selected, the End Shift folder will be created, and the End Shift files will be stored. This option is “on” by default. If off files will not transfer to drive.
- **Keep only updated databases-** If this option is selected, any databases that were not updated during Begin Shift will be considered outdated and removed. This option is “off” by default.



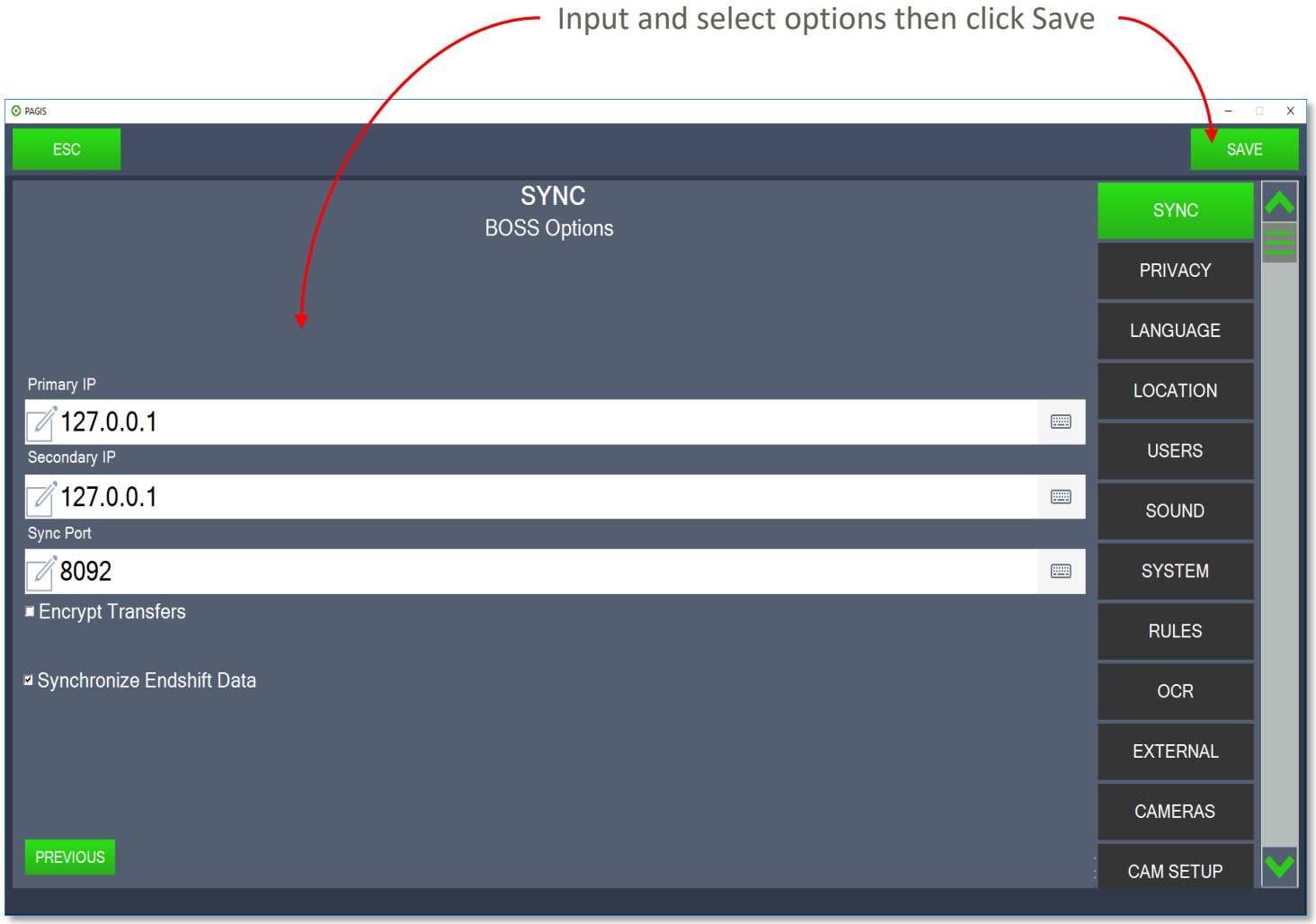
Copyright © 2021 Neology, All Rights Reserved.

Sync-Boss

Synchronization to Boss:

If choosing to establish BOSS as the synchronization method, PAGIS must have a network connection to successfully communicate with BOSS. You must also have an IP address of the BOSS server that is reachable via TCP/IP port 8092.

- **Primary IP-** Enter IP or Domain name of Boss server, used for primary network connection. PAGIS utilize TLS-1.0 as its communication security protocol.
- **Secondary IP:** Enter IP or Domain name of Boss server, used for alternate network connection if switching from Cellular to Wifi. Leave default or clear if not utilizing.
- **Sync Port-** Default port is 8092, this port can be customized but you must make sure the Boss “RestAPI” port matches the new custom port.
- **Encrypt Transfers-** If this option is selected, the end shift files created by the PAGIS Software will be encrypted. This option is “off” by default.
- **Synchronize End Shift Data-** When selected all Read/Hit data will be synchronized with Boss during its automatic communications cycle and during manual End Shift.



Copyright © 2021 Neology, All Rights Reserved.

Privacy

Privacy settings ensure data compliance and prevents locally storage data from filling up local disk space. These configurable settings control the length of time in days, hours, and minutes that Reads, Hits, Local Alert List and Audit information is to be saved locally.

- **Never-** Privacy Settings disabled.
- **On Startup-** With On Startup selected, each time PAGIS is started, it checks privacy settings and evaluates whether existing information has exceeded the allowable age.

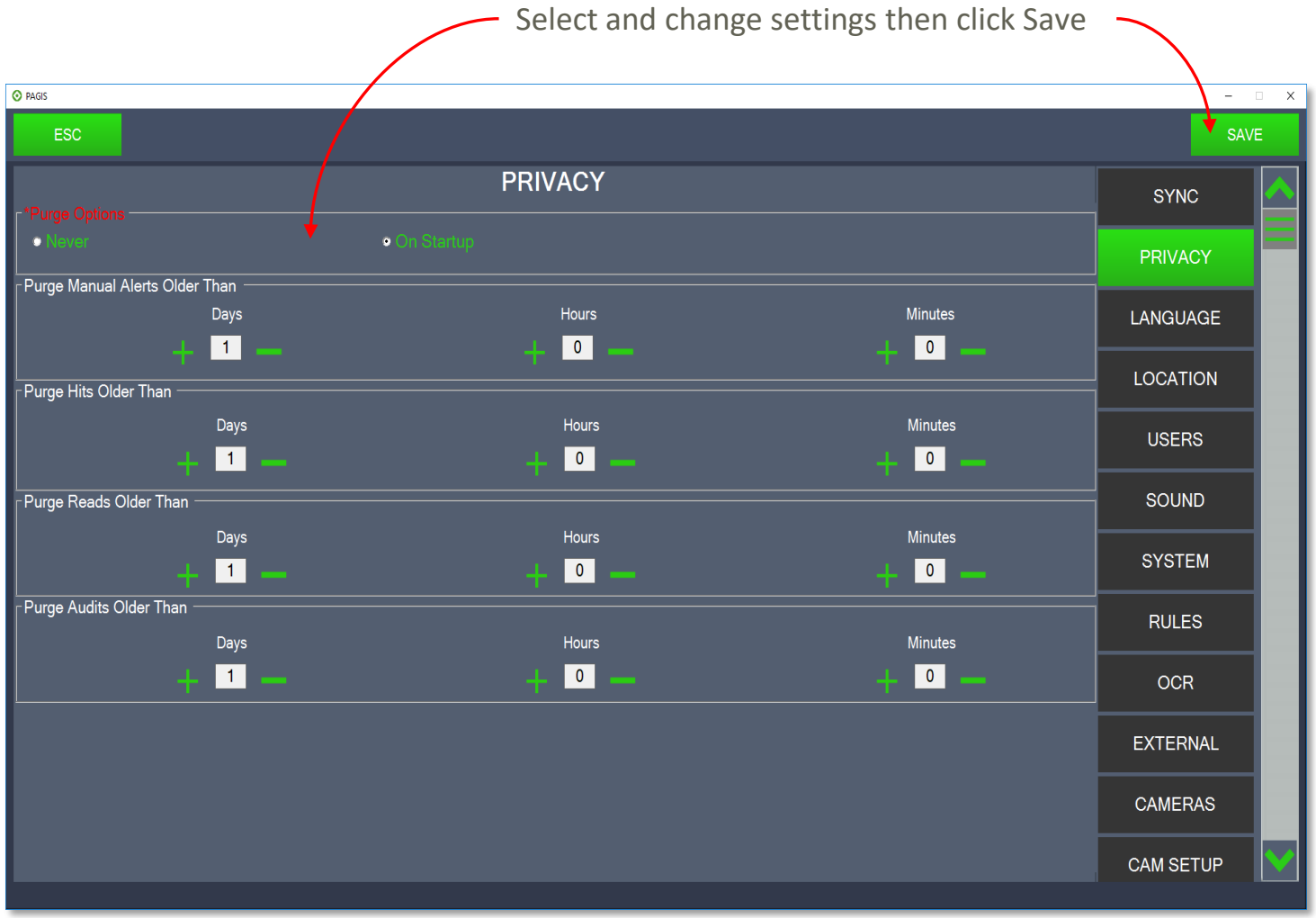
Purge Manual Alerts Older Than:
Control how frequently the Alert List databases stored on PAGIS is purged. Purging occurs when the timestamp on the Alert List exceeds the retain settings. This setting applies to all Alert List, but Alert List deployed to PAGIS by BOSS will be re-synchronized.

Purge Hits Older Than:
Control how frequently the Hits stored in the PAGIS Software are purged. Any Hits exceeding the specified duration will be purged from PAGIS.

Purge Reads Older Than:
Control how frequently the Reads stored in PAGIS are purged. Any Reads exceeding the specified duration will be purged from PAGIS.

Purge Audits Older Than:
Controls how frequently Audits are purged from PAGIS.

If PAGIS Sync is set to BOSS, purging will not apply to data that has been synchronized.

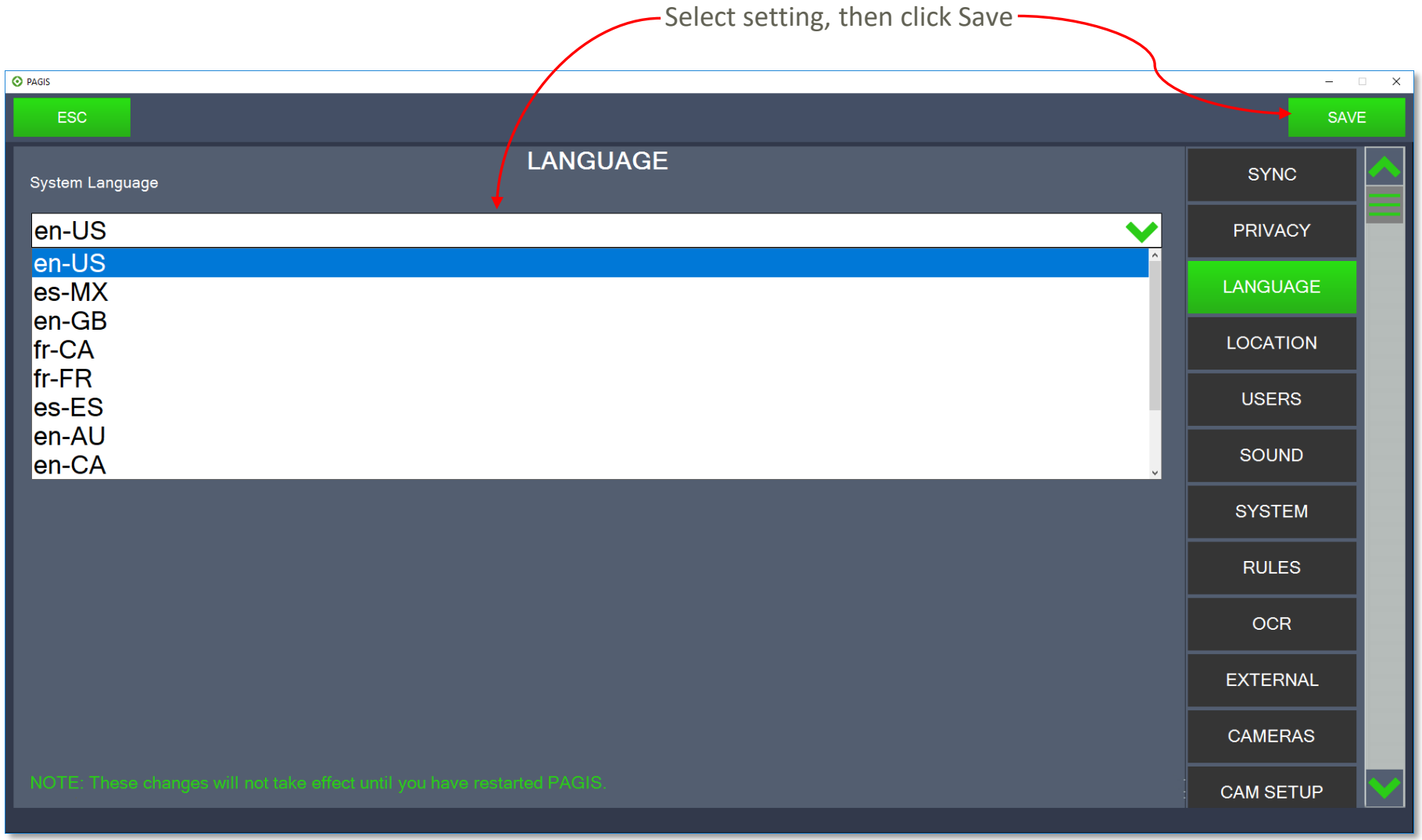


Note: Once Reads and Hits have been sanitized, they can no longer be viewed in PAGIS.

Copyright © 2021 Neology, All Rights Reserved.

Language

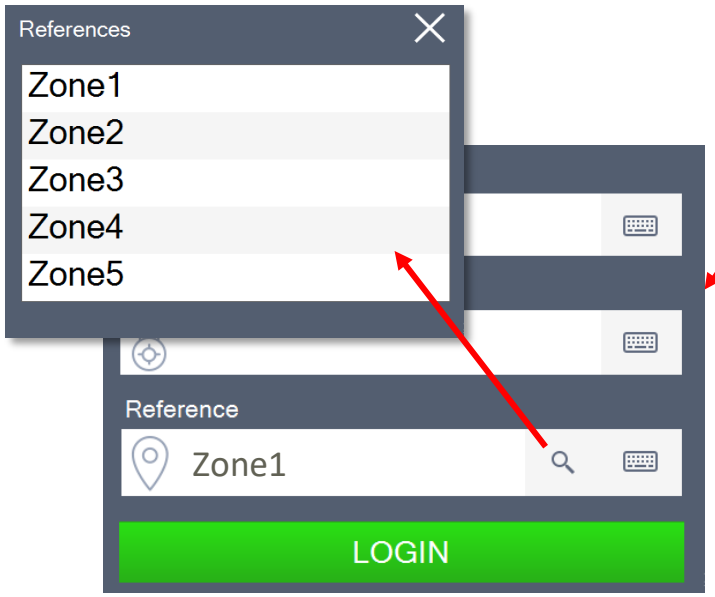
Language- Change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down menu, Change are applied after PAGIS restart.



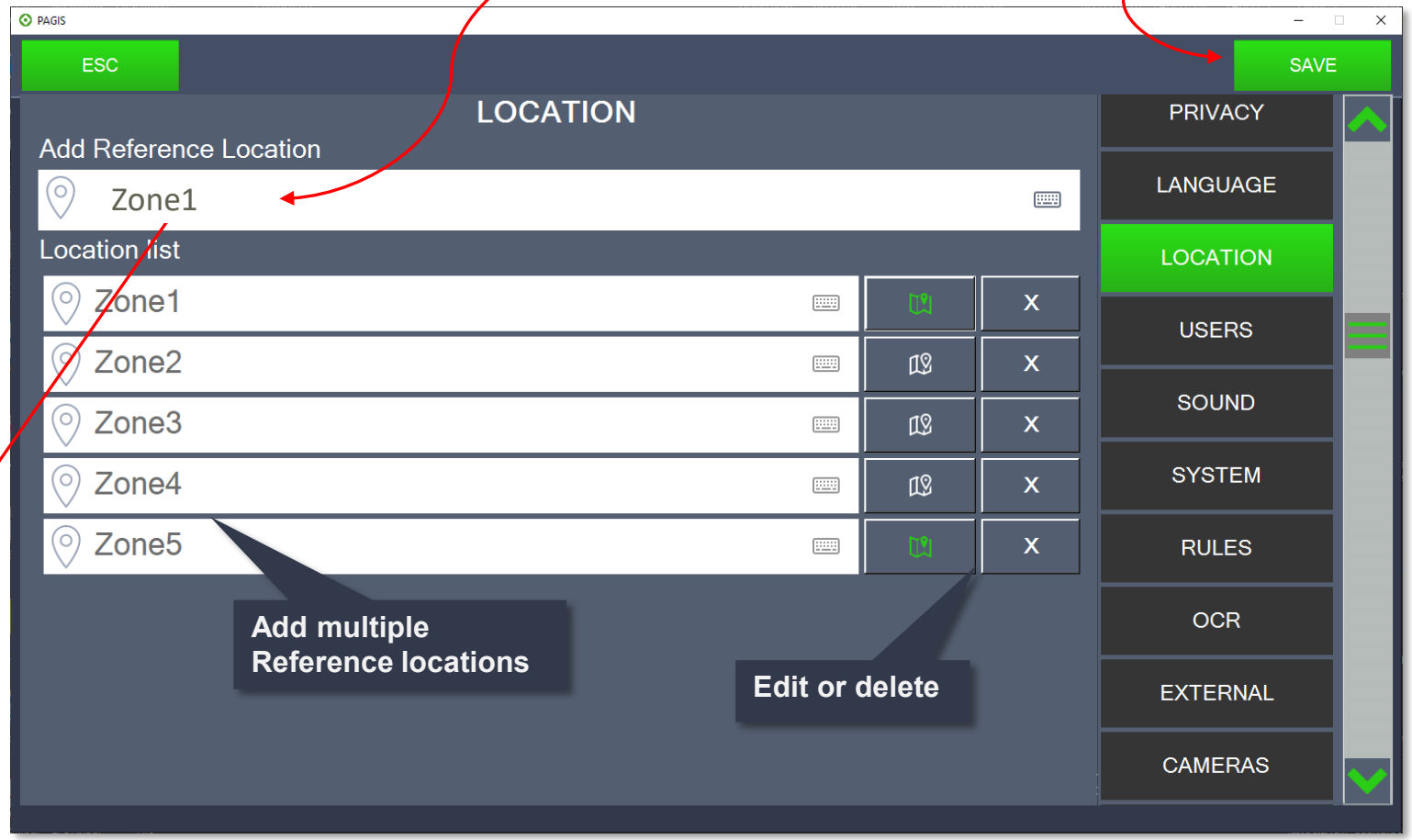
Copyright © 2021 Neology, All Rights Reserved.

Reference Location

Reference Location- Any name entered in the reference field is listed as the default system location at the login screen. The location name will be assigned with every Read/Hit capture by PAGIS, this information is not tied to the GPS location.



Reference listed at Login Screen



Copyright © 2021 Neology, All Rights Reserved.

Users

IMPORTANT: Adding new users through the PAGIS Software should be limited to those customers who are not syncing to the Back Office System Software as BOSS will override any users added manually during the next sync.

User – Add a new user. The username field will accept up to 15 alphanumeric characters.

Password – Enter a password to associate with the username. The password field will accept up to 15 alphanumeric characters.

Privileges – Select the privileges associated with the user by, active privileges turn green.

- **Sync** – Allows the user to synchronize files.
- **Ext** – Allows the user to import external Alert List.
- **Adm** – Allows the user to access PAGIS Settings.
- **Del** – Remove a user from the list. Click “DEL” (Turn Green”), click “SAVE” to delete.

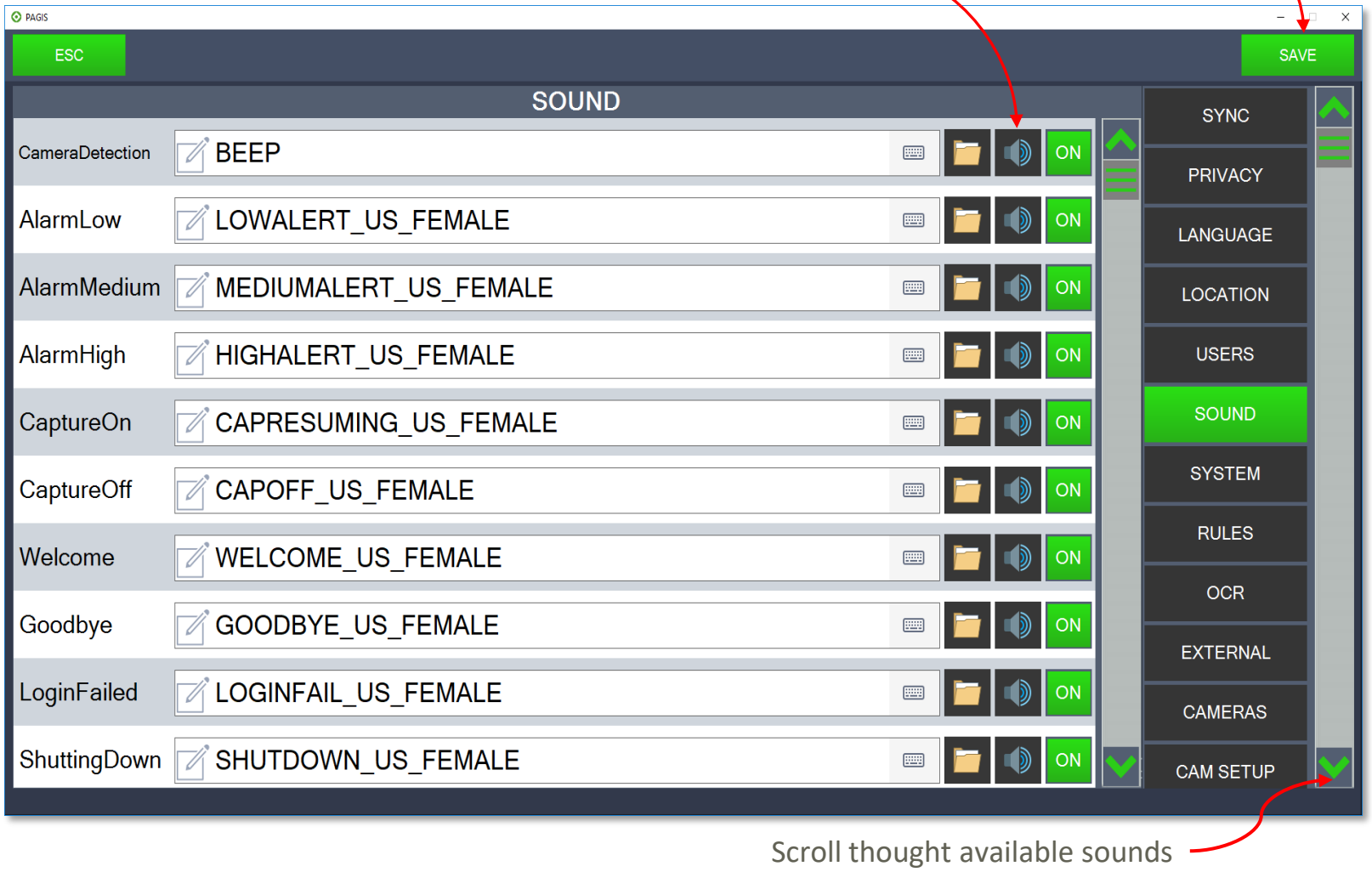


Copyright © 2021 Neology, All Rights Reserved.

Sounds

The Sound screen associates available sound files with specific alerts and actions.

- **On or Off-** Sounds are active when the button is On (green) and deactivated when the button is Off (red).
- Choosing sounds is an optional feature. Sounds are preset in the PAGIS Software and may be modified by an Administrator. By default, the PAGIS Software will play a sound to notify the user when an event or "Hit" is triggered. Sound files (.wav file format) are stored in the Sounds folder in the PAGIS Software directory.
- To select new sound files, select  button to open Windows File Explorer.
- All sound changes are Global and apply to all uses in PAGIS.
- Scroll bar thought available options.



Copyright © 2021 Neology, All Rights Reserved.

System

The System screen determines configurations for Auto login, GPS connection and custom camera resolution.

- **Auto Login-** This feature enables PAGIS to forgo prompting user to login. This feature is helpful for unattended use such as speed-trailer applications and with “drop and go” deployments.
- *Note: Deployed uses from BOSS must be stopped for Auto Login to work.*

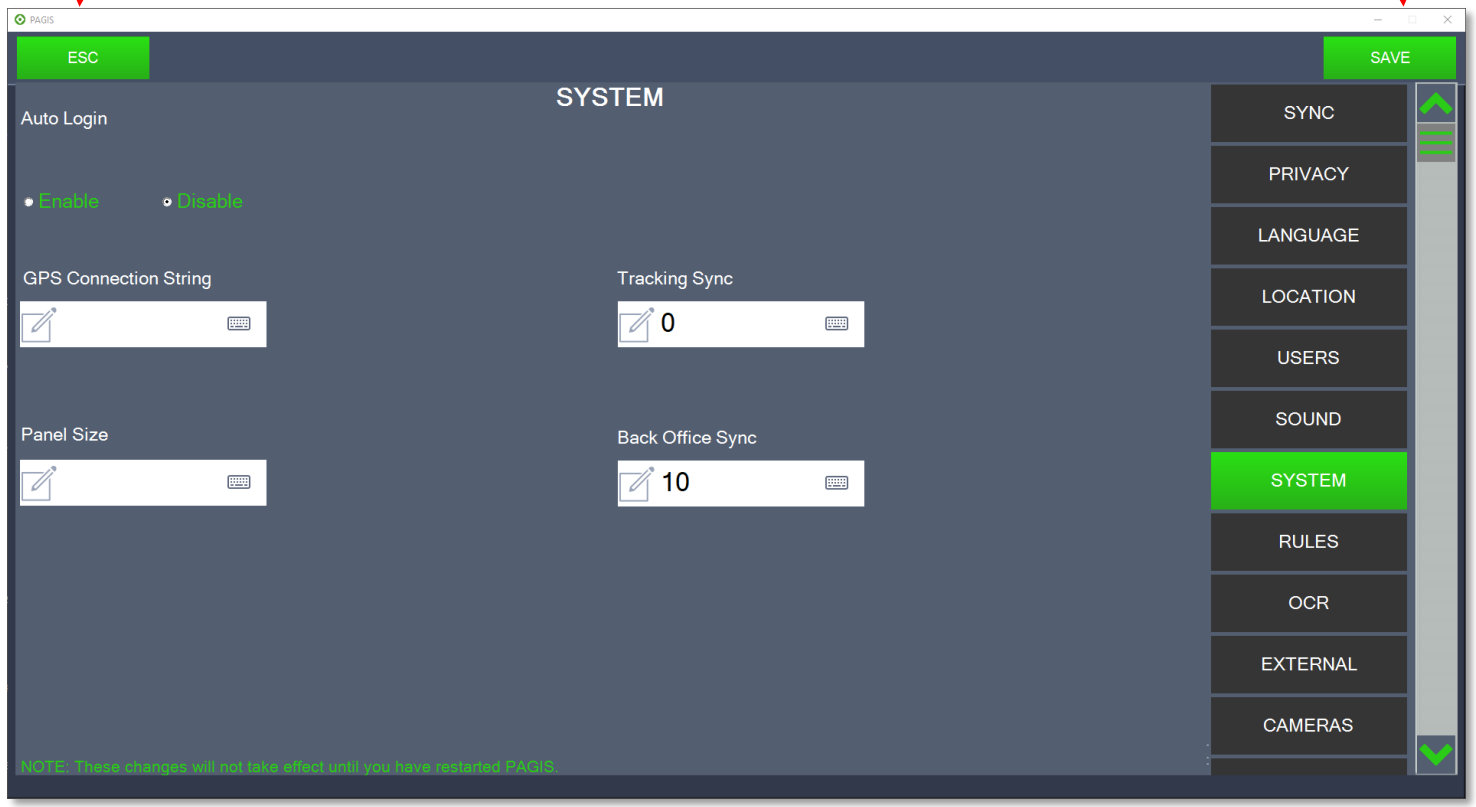
- **GPS Connection String-** The GPS string is utilized to redirect PAGIS to acquire GPS feed from different source. Defaults for PIPS ALPR system are no entry for MDC installed PAGIS and 6 for Standalone version. The GPS connection string defaults to a COM port value, although it may also refer to TCP/IP: Port option if IP is included in the connection string, example (127.0.0.1:8080).

- **Panel Size-** This feature controls the color image resolution PAGIS displays in the camera panels in Main View screen. By default, PAGIS controls the aspect resolution. Custom resolutions may be entered to help with non-standard screen size to fill in the spaces. Value format is Width x Length.

- **Tracking Sync-** Controls the sync intervals in (Sec.) that PAGIS communicates with Boss4 to update tracking status. Default off=Zero, values can range from 1-9999.

- **Back Office Sync-** This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

Click Save to apply changes or Esc to return to the previous screen and cancel any modifications.
Restart PAGIS Software to activate any changes.



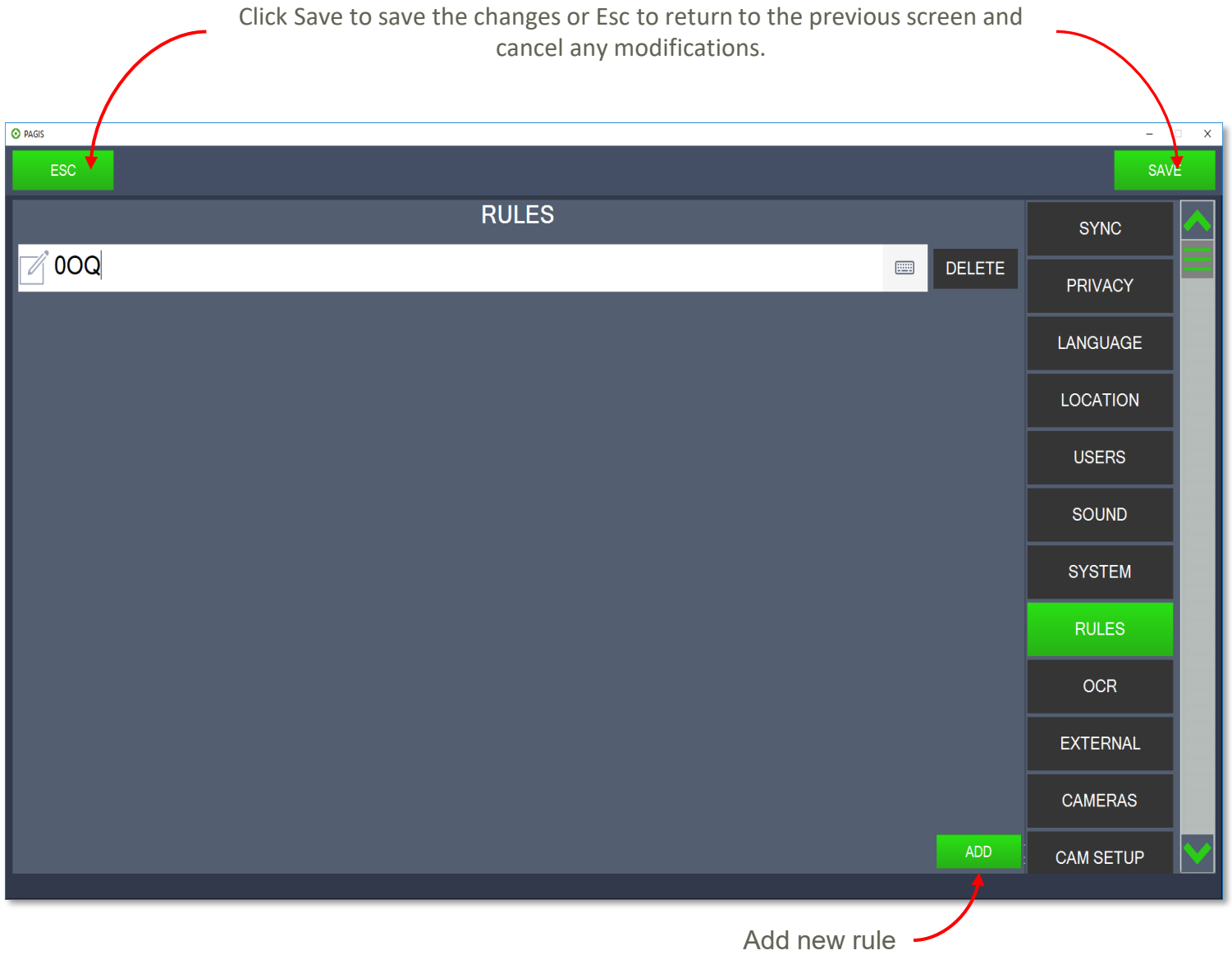
Copyright © 2021 Neology, All Rights Reserved.

Rules

Rules provide a way to check for commonly misread character by creating a set of rules for checking against available Alert List. For instance, “8” and “B” are sometimes mistaken. If the OCR engine reports a plate as ABC123, you might want PAGIS to check both ABC123 and A8C123 against all Alert List to find a match. While PAGIS is less likely to miss a Hit, the process can also produce more false Hits.

Add a new Rule:

- **Add-** Click Add and enter a single character instance (the letter “O,” for example), and enter a list of similar characters (letter “O”, number “0”, and letter “Q” in this example).
- With this rule defined, anytime the system Reads an “O”, it will run the query for matching purposes as “O”, “0”, and “Q”.
- **Delete-** Click and highlight the “Delete” button then save to delete a rule.
- **Save-** Click to save changes.



Copyright © 2021 Neology, All Rights Reserved.

OCR

Click Save to save the changes or Esc to return to the previous screen and cancel any modifications.



The OCR screen is used to enable inverse and square plate Reads, to disable duplicate plate Reads and control image output. Each check box toggles the options: if a check mark appears, the option is active. If the box is empty, the option is disabled.

JPEG Images- Use compressed .jpg images instead of full-resolution bitmaps. On by default. When this feature is activated, it minimizes storage requirements for collected data.

Inverse Plates- This feature can be useful for plates with a dark background and light lettering. Off by default. This option increases the processing load and therefore should remain disabled until it is needed due to the region.

Square Plates- Adjusts the Read area for plates that are square instead of rectangular. Off by default.

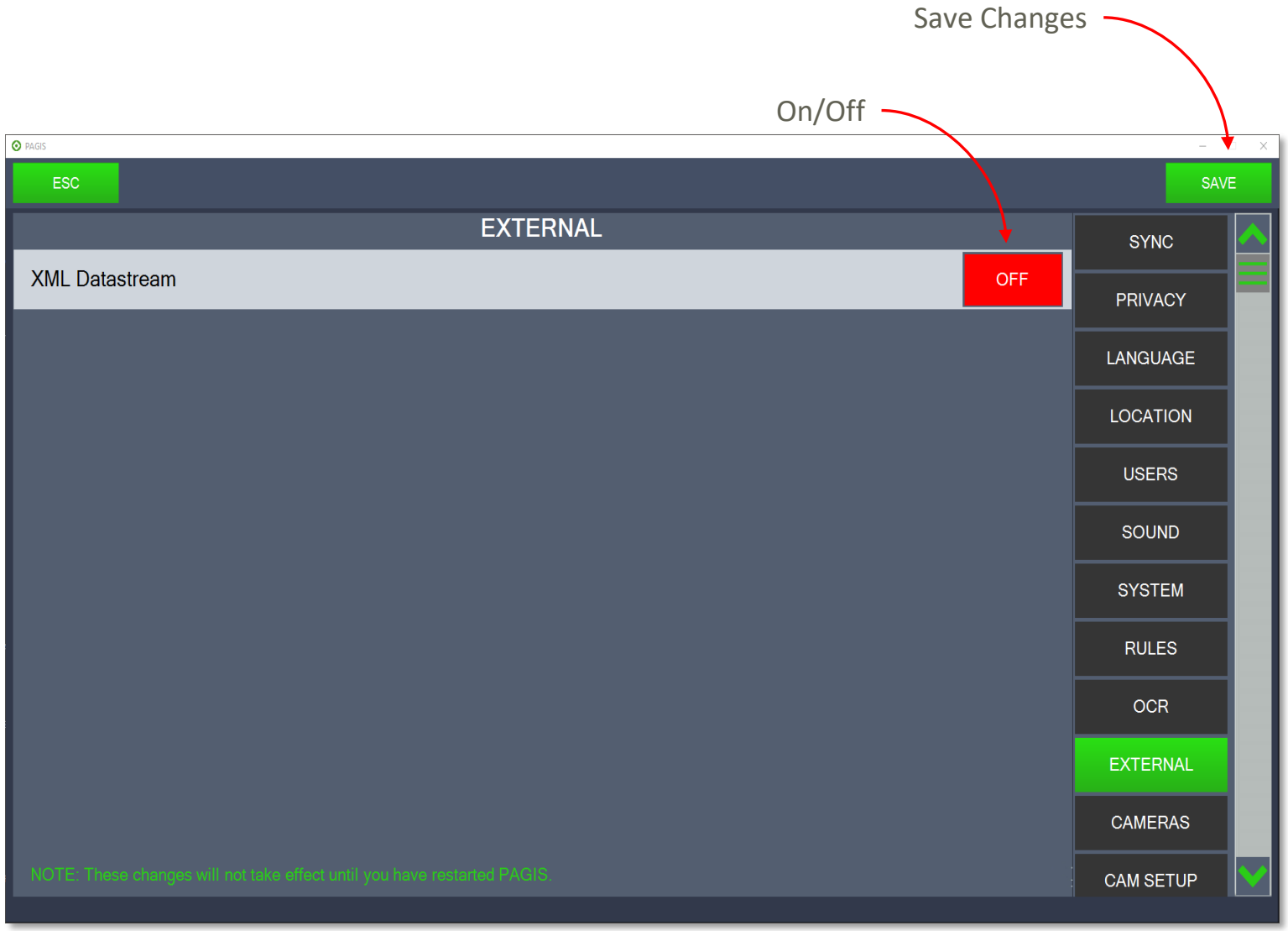
Disable Duplicate Read- Turns off duplicate Reads. If the same plate is Read by more than one camera within a short time frame (4Sec), the duplicate is ignored. This minimizes storage requirements for the collected data and improves system metrics related to the number of Reads, on by default.

Copyright © 2021 Neology, All Rights Reserved.

External

The PAGIS datastream can be used to Read current data from a running PAGIS system. The data available via the datastream includes Reads, Hits and images. The connection to the datastream is TCP/IP (default port: 10100). Metadata is passed in real time and images are pushed periodically.

- To make this connection, click the red OFF button to change it to a green On button and then press Save. Any changes made on this screen will take place after the PAGIS Software is restarted.
- PAGIS Manual has detailed connection protocol and XML header format information.



Copyright © 2021 Neology, All Rights Reserved.

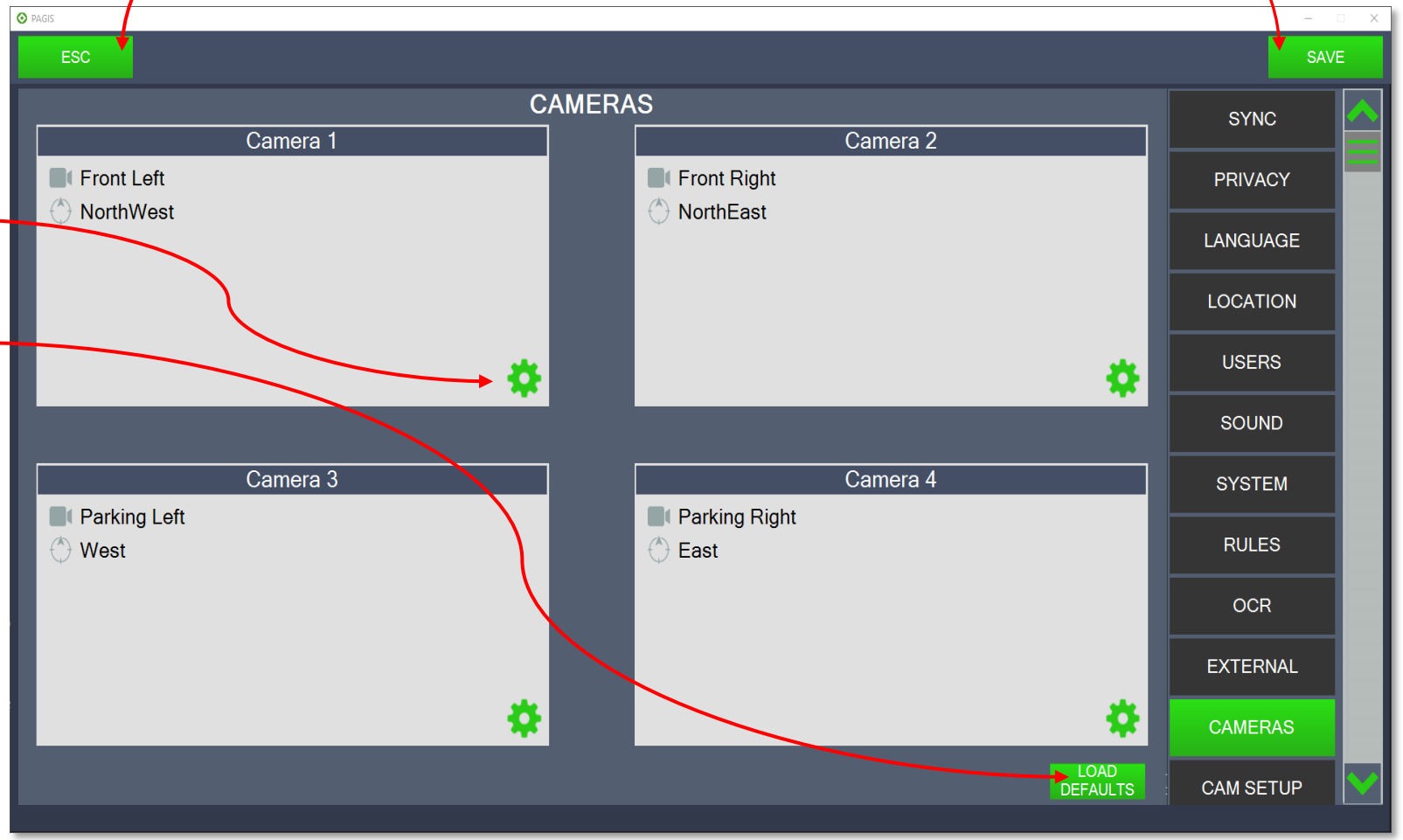
Cameras

Click Save to apply changes or Esc to return to the previous screen and cancel any modifications.

The Camera setting panels are a software representation of the physical camera ports located on the mobile processor. Each camera panel has its own unique settings that can be altered to accommodate custom application.

- **Camera Settings-** Edit camera name, location reference symbol, mobile device type, video capture path and OCR utilization.
- **Load Defaults-** Loading a default setting provides a baseline configuration reset and is based upon a standard four- camera system. Choosing default removes all existing Camera & Configs settings and resets them to factory default.

Pro Tip- When entering the “Cameras” settings PAGIS will initialize a confirmation check with the mobile process for existence. If the connection check fails PAGIS will report a “Could not connect to remote host!” message then proceed to load camera setting panels with no values, if this occurs double check and make sure all communication requirements are meet for PAGIS and mobile processor.



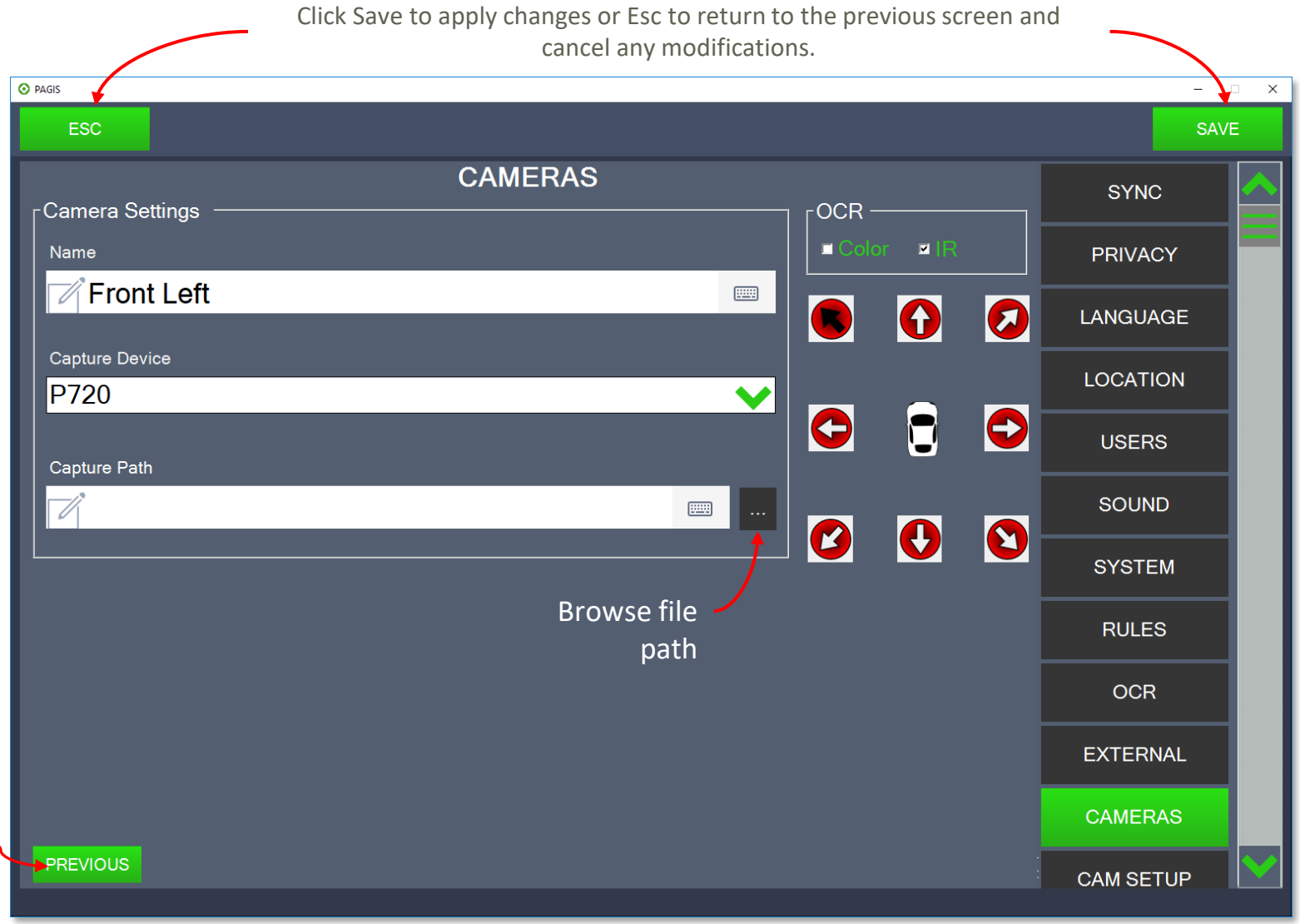
Copyright © 2021 Neology, All Rights Reserved.

Cameras Settings

Edit Camera Settings

Change the below setting as needed, PIPS camera setting are pre-loaded and typically do not need alterations.

- **Name-** The Camera Name field accepts 50 characters, but PAGIS will only display 11 characters on the Main View screen.
- **Capture Device-** The connected mobile processor delivers the device type to PAGIS when entering the “Camera” settings section, options are P720 for SX4e and P442 for SX4 models.
- **Capture Path-** Configure PAGIS to aspect video feed from video file, AVI files only.
- **OCR-** Active OCR for Color or IR or both.
- **Camera Position-** Symbol indicator for alert screen to indicated camera placement direction.



Copyright © 2021 Neology, All Rights Reserved.

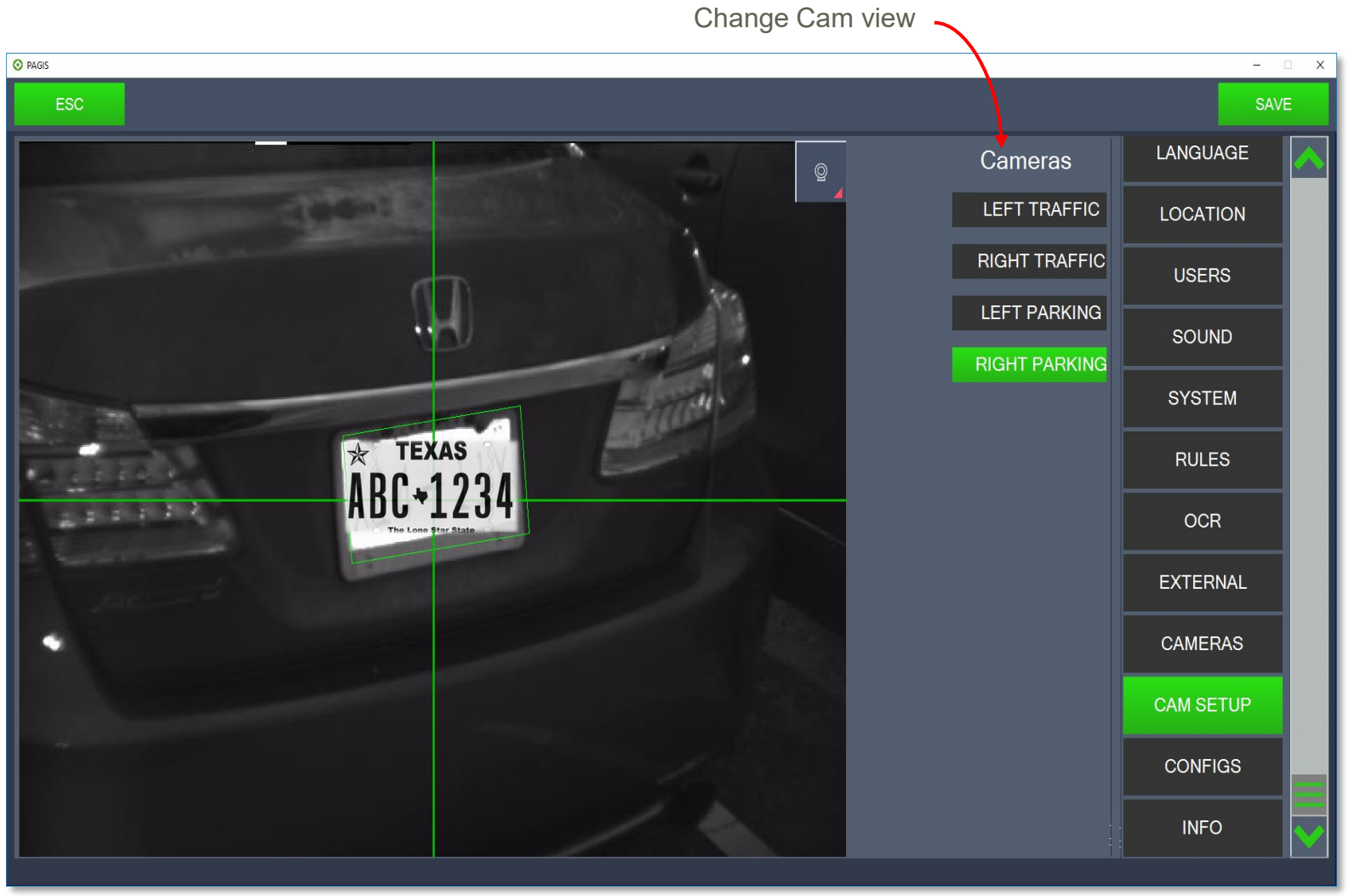
Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows for switching view modes from Color to IR to ensure the system is functioning properly and to assist in camera alignment.

Cam Setup Features:

- **Alignment Grid-** The alignment grid provide a basis for camera alignment based on placement.
- **Color View-** The Color View Mode is the default view when entering Cam Setup. This displays a live preview of the color camera video feed.
- **IR View-** By clicking on the Camera View Selector button, this will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera video feed.

NOTE: Typically, the IR camera is performing the plate analyses for capture. It is recommended to align the cameras using the IR video feed.



Copyright © 2021 Neology, All Rights Reserved.

Configs

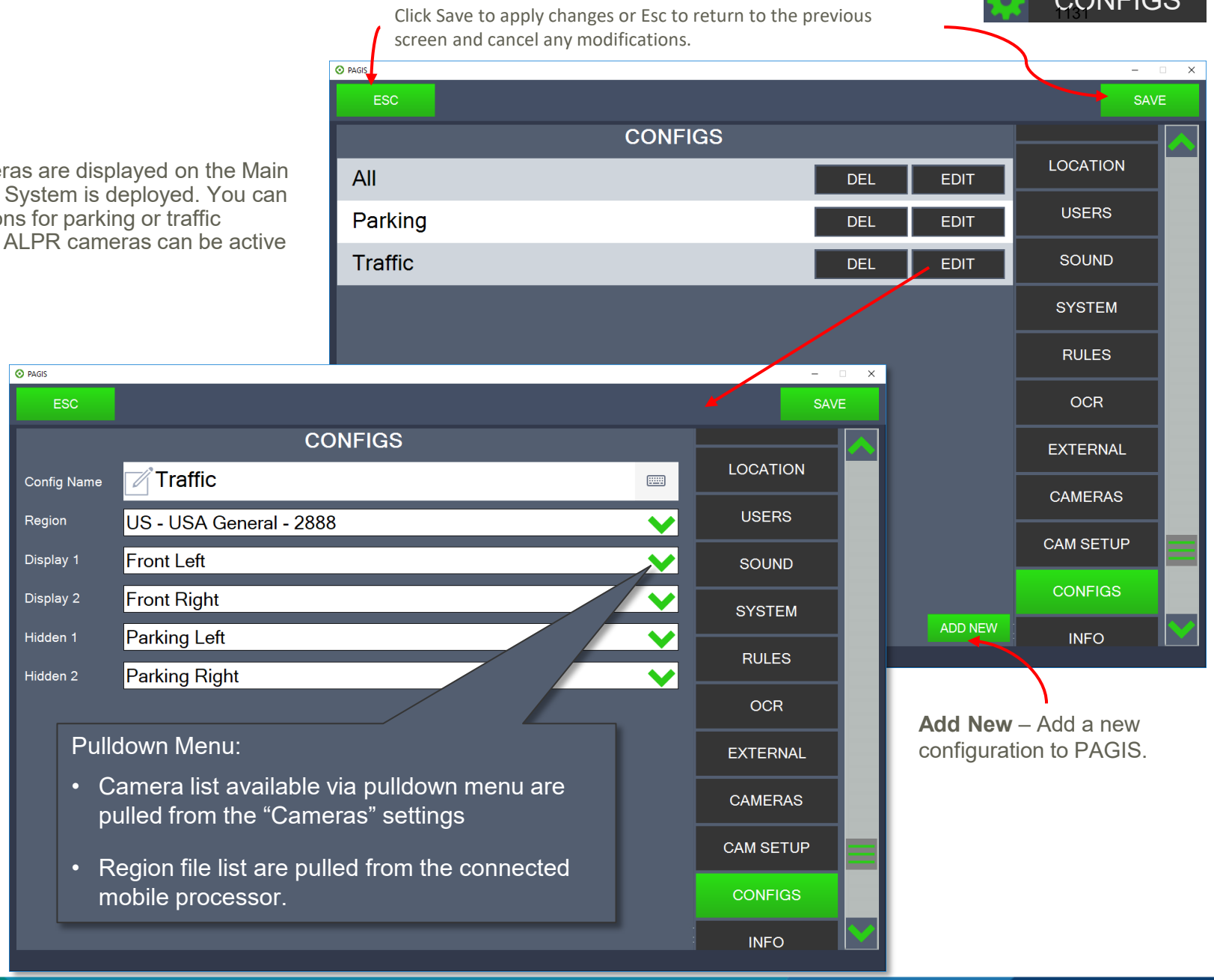
The Configs screen allows you to define how the configured cameras are displayed on the Main View screen and to set the region of the country where the Mobile System is deployed. You can also use the Configs screen to set up multiple camera configurations for parking or traffic monitoring to replicate a particular driving environment. Up to four ALPR cameras can be active in each mode.

Config buttons:

- **Del** – Removes the current configuration from the PAGIS Software.
- **Edit** – Opens the Edit Configs screen where you can modify settings for the selected configuration, including selecting a region and selecting which cameras to display or hide.

Configs Settings:

- **Config Name-** The name of the configuration mode.
- **Region-** Select region file to be used, these are preloaded at time of purchase. This setting must be applied on first setup or cameras will not capture data.
- **Display 1-** This camera is always displayed on the left-hand side of the Main View screen.
- **Display 2-** This camera is always displayed on the right-hand side of the Main View screen.
- **Hidden 1 and 2-** When populated, these cameras are functioning and performing OCR, but the images are not visible to the user. Hits and Reads will still be generated by these cameras and alert still notify users.



Copyright © 2021 Neology, All Rights Reserved.

INFO

PAGIS Information:

- PAGIS version and ORC engine versions.
- Technical Support email address.
- Neology offices and phone numbers.

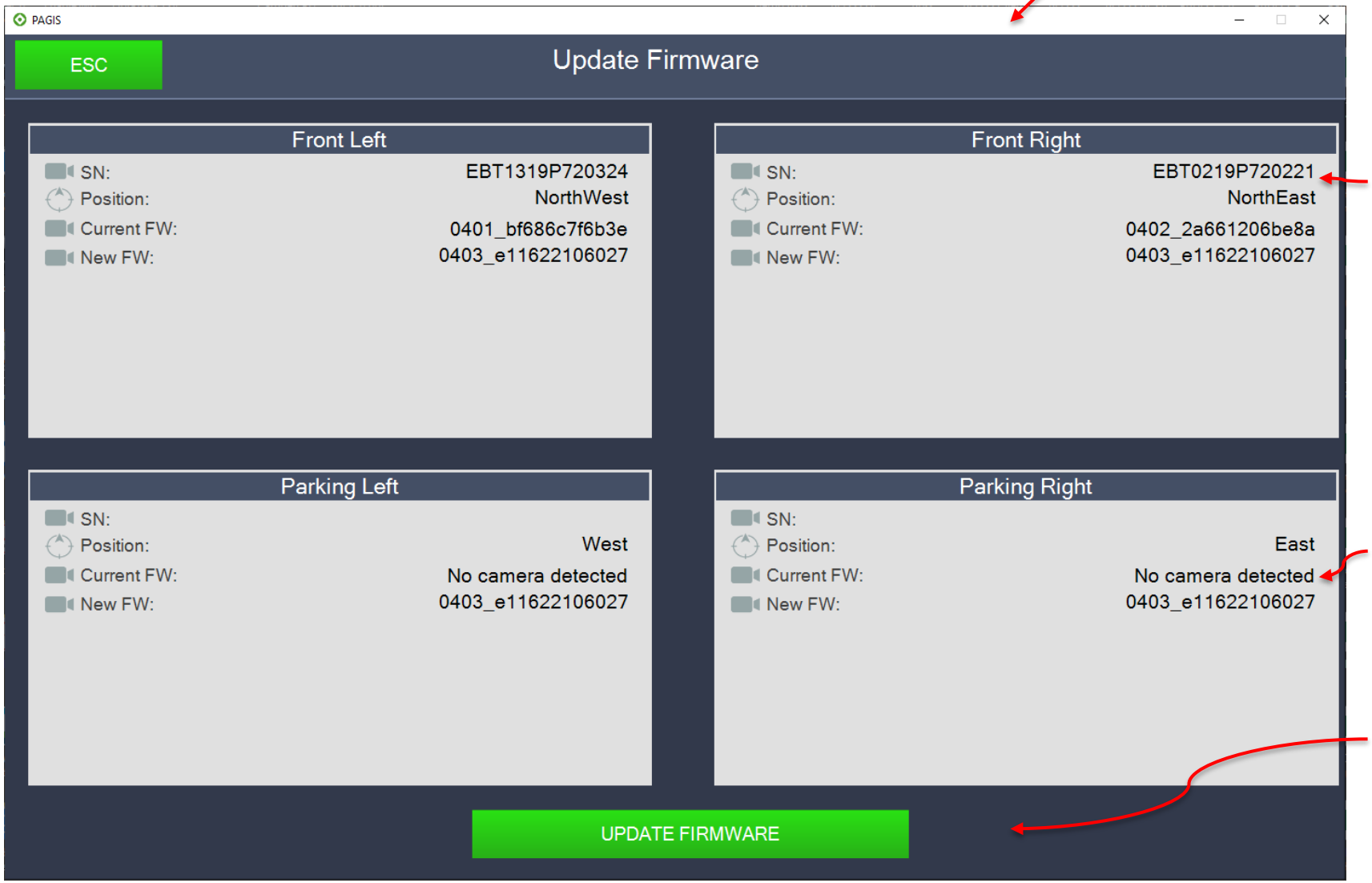


Copyright © 2021 Neology, All Rights Reserved.

Camera Firmware Update

(Admin Users)





Camera firmware updates provides a means for PIPS to update the camera software to enhance and or correct camera performance.

Firmware Updater Window List.

- Camera serial number.
- Position.
- Current FW version,
- New FW version available.

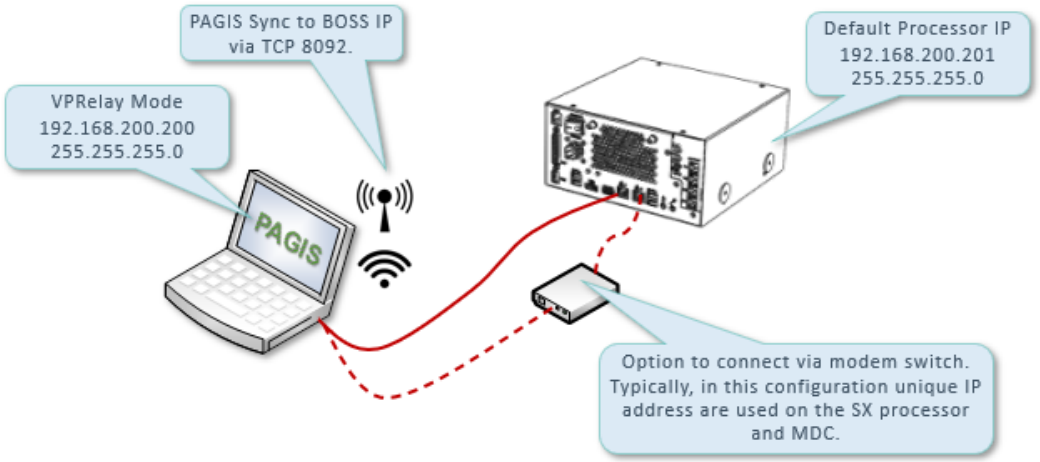
The firmware update process only updates camera that are attached and function on the mobile processor.

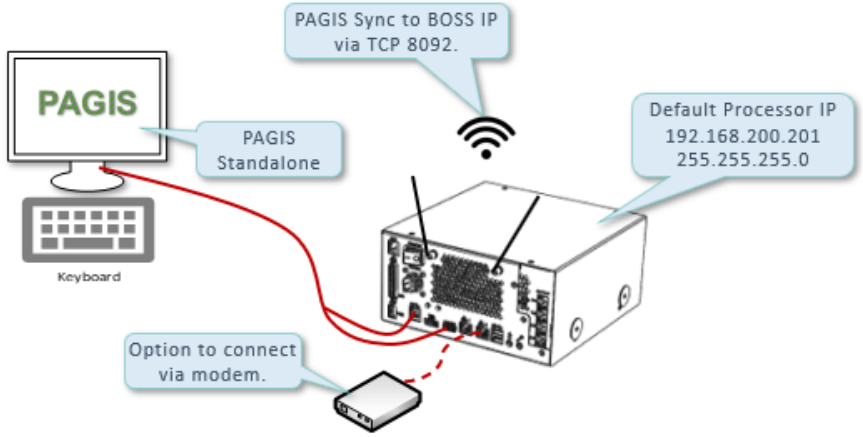
Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and can not be interrupted or risk permanently damaging the cameras.

Copyright © 2021 Neology, All Rights Reserved.

PAGIS

Operation Mode Requirements Installation



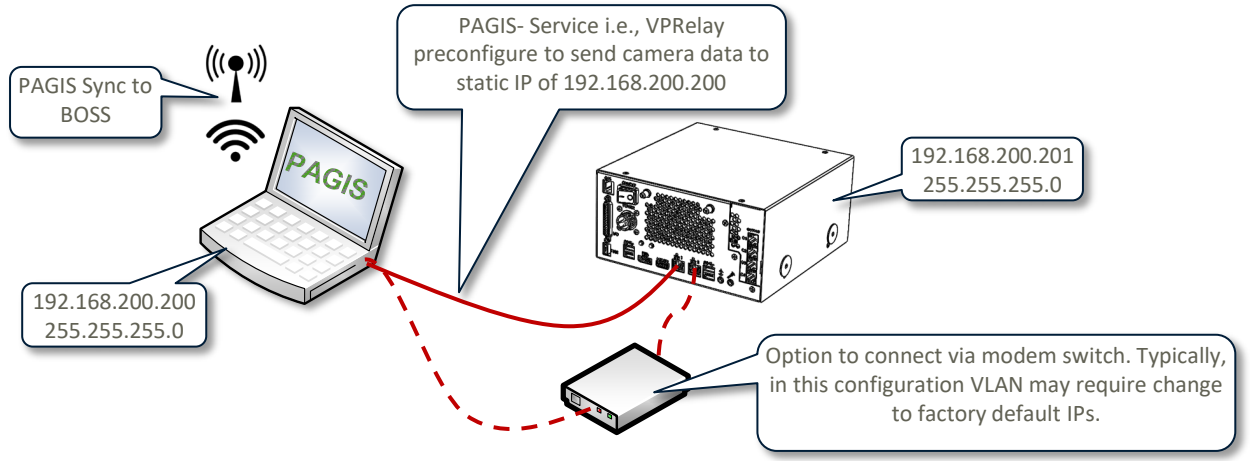


Copyright © 2021 Neology, All Rights Reserved.

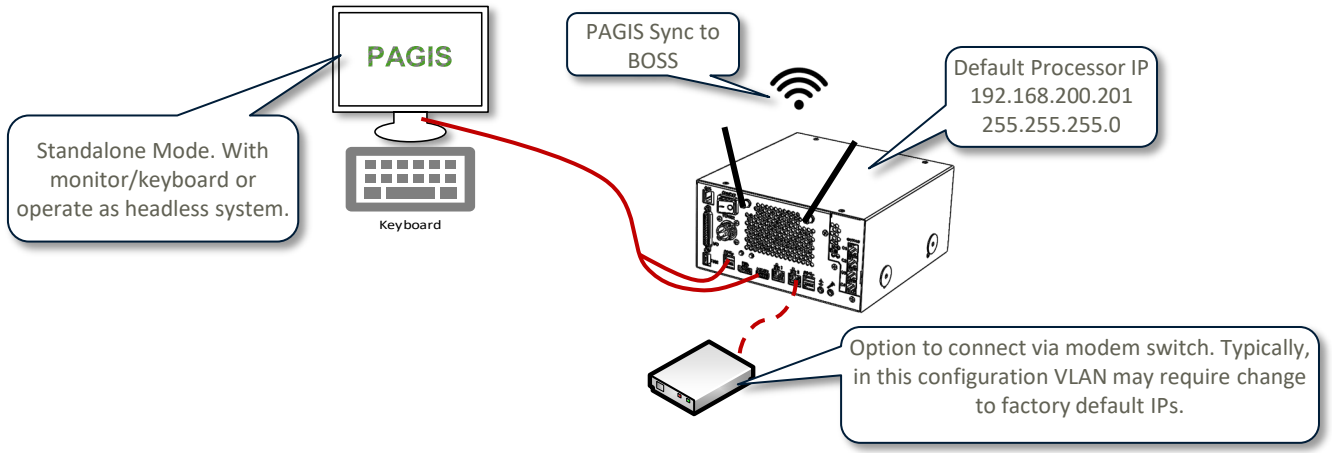
PAGIS Operation

PAGIS Operation Modes
The Neology ALPR Mobile SX Processor can be configured in two distinct ways.

Client/Server (VPRelay) Mode
The Client/Server configuration consists of a Mobile ALPR Processor, up to four ALPR cameras with mounting brackets, and a network connection to a Mobile Data Computer (MDC)/laptop in the front of the vehicle. The ALPR processor collects images and data for license plate recognition and relays it to the MDC over a static network connection. The primary advantage of the Client/Server configuration is that it allows a user to be notified of “alerts” while operating the vehicle. This is done through mobile ALPR software called “PAGIS” running on the laptop/MDC and displaying the ALPR data inside the vehicle.



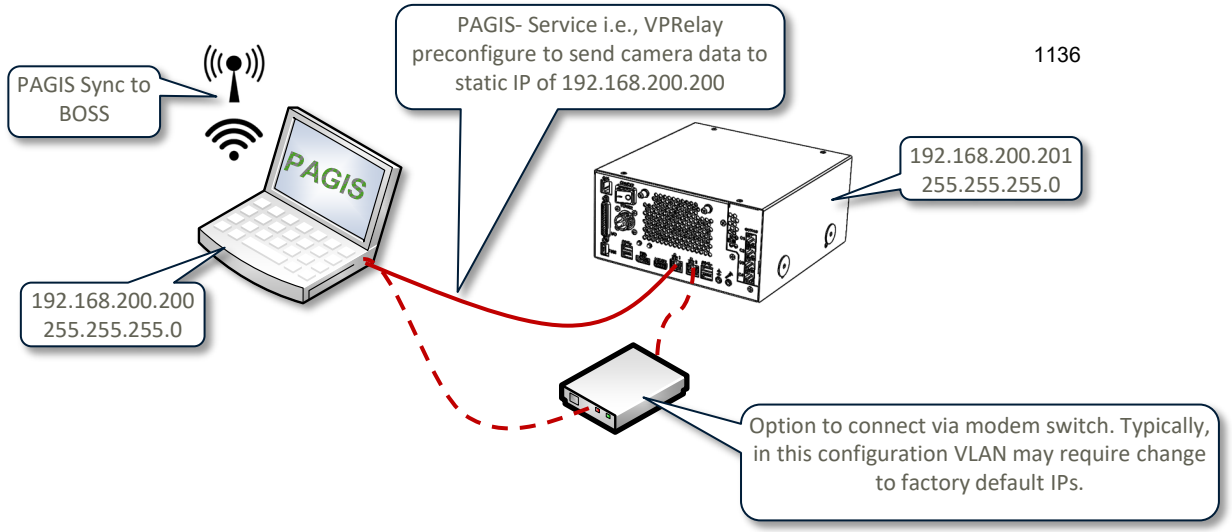
Stand-Alone Mode
The Stand-Alone configuration consists of a Mobile ALPR Processor, up to four mounted ALPR cameras, and a touchscreen monitor. The self-contained system performs all plate recognition and runs its own copy of the PAGIS software. The primary advantage of the Stand-Alone configuration is its deployment flexibility as it does not require the agency to own and maintain MDCs/laptops. Some utilization examples are speed trailers, parked covert vehicles, or in manned patrol units (when equipped with touchscreen monitors and a hotspot/cellular data network).



Copyright © 2021 Neology, All Rights Reserved.

PAGIS Prerequisites

Mobile Data Computer (MDC)



PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings (MDC):

Neology's mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the mobile processor your computer must adopt 192.168.200.200 for the MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the .200 IP address, using alternative IPs on Laptops will result in the software’s failure to communicate with the cameras unless further change are made on the mobile processor, see PAGIS manual.

Copyright © 2021 Neology, All Rights Reserved.

PAGIS Installation

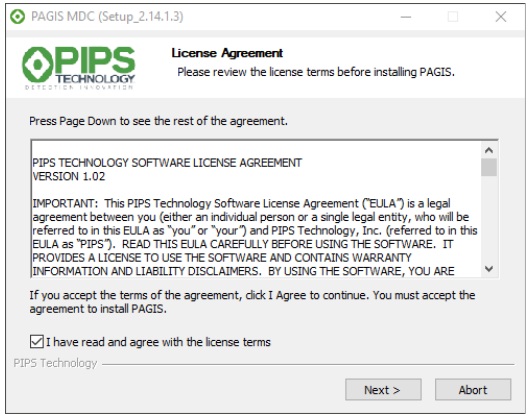
Mobile Data Computer (MDC)



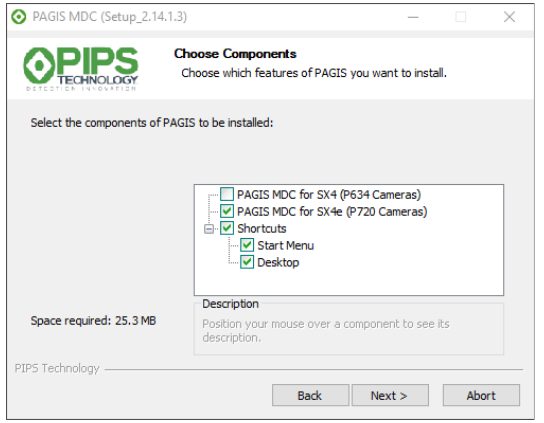
4. Place the PAGIS installer on your computer's desktop, "PAGIS_Setup_MDC_2.14.x.x.exe".
5. Right click the PAGIS installer executable and select "Run as administrator".

PAGIS Software Installation (MDC)

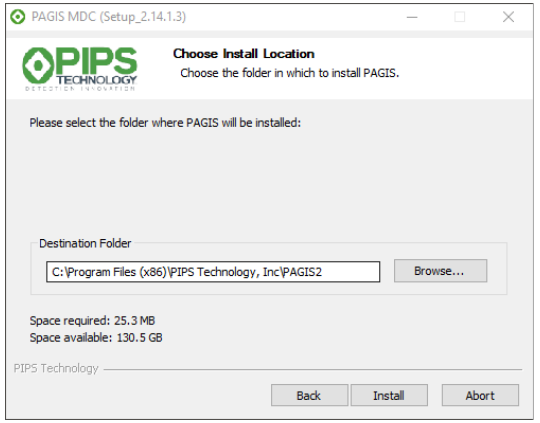
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you "EndShift" any existing data, then uninstall PAGIS.
2. It is recommended you "EndShift" any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor, if the 4 camera IO ports are vertically arranged RJ45's then it's a SX4e, if they are vertically arranged circular shaped "LEMO" connectors then it's a SX4. Horizonal arranged circular shaped "LEMO" connectors are SX3 and is not compatible with PAGIS 2.14.



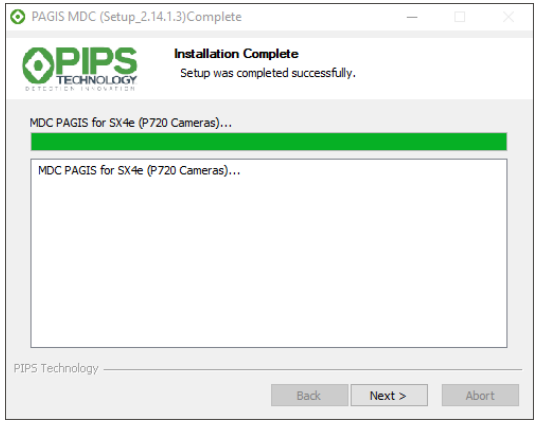
6. Check the license agreement box, then click Next.



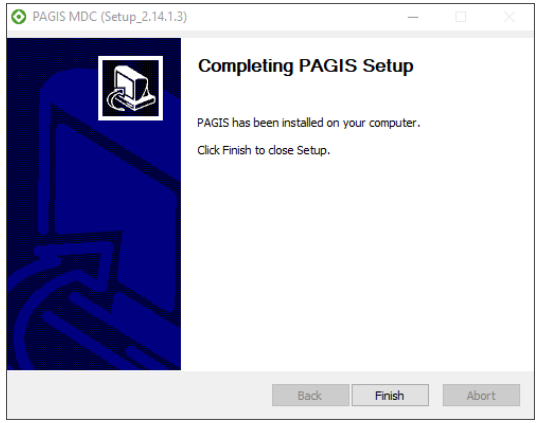
7. Select the mobile processor type and alter "Shortcuts" if needed. Next to continue.



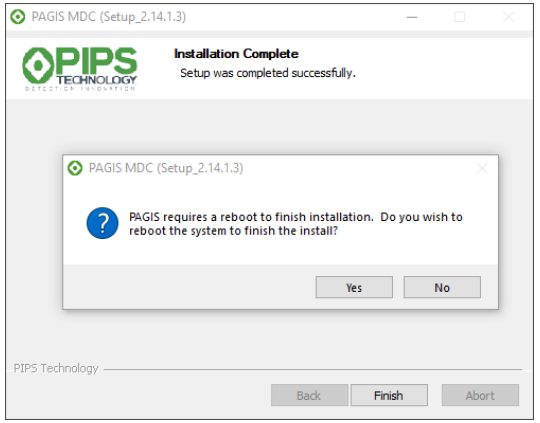
8. Confirm path if upgrading, click Install to proceed.



9. Installation Compete, Next to proceed.



10. Click Finish.

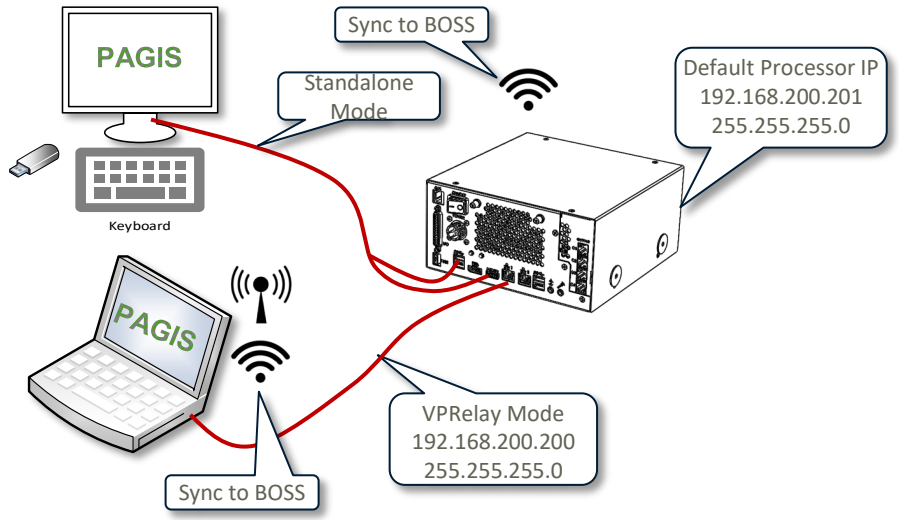


11. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

Copyright © 2021 Neology, All Rights Reserved.

PAGIS Updater

Mobile Processor, SX4 & SX4e

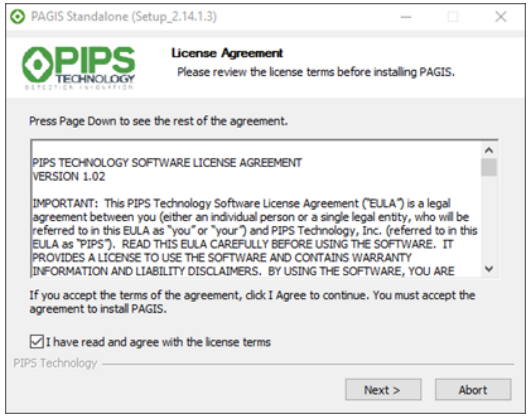


PAGIS Software updater (Mobile Processor)

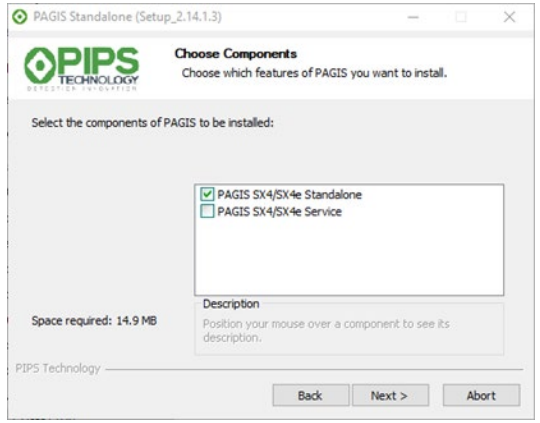
- PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
- The PAGIS updater only updates existing versions of PAGIS that reside on the mobile processor, version 2.9 and newer.
- Update required for both “Standalone” & “VPRelay” to support some of the newer features.
- The processor must be in its respective mode to update that option as the folder paths are hidden when not active, see “Change Mode” in SX4 or SX4e manual.



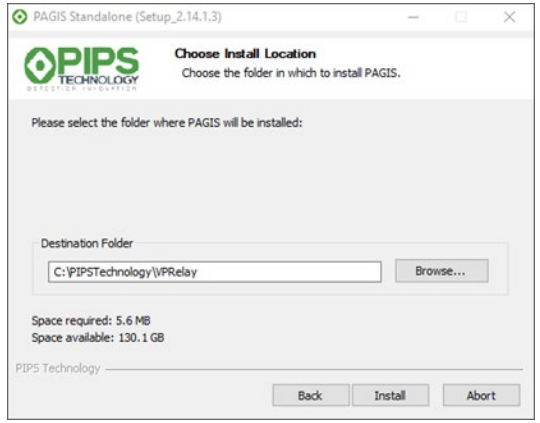
1. Remote desktop into processor or utilize attached monitor/keyboards with USB drive.
2. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
3. Execute PAGIS Updater.



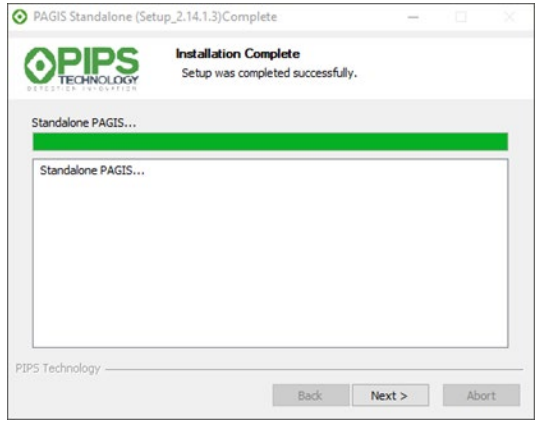
4. Check the license agreement box, then click Next.



5. Select option to update, next to continue.
- Standalone= PAGIS login from Processor.
- Service= PAGIS login from Laptop..



6. Change the default path presented by updater, see below.
- For “Service” C:\PIPSTechnology\VPRelay
- For “Standalone” C:\PIPSTechnology\Standalone



7. Installation Compete, Next to proceed.
8. Click Finish.
9. Click Yes to reboot.

Copyright © 2021 Neology, All Rights Reserved.



Thank you

Copyright © 2021 Neology, All Rights Reserved.