From: Richard Porro
To: Bank Robbery
Cc: John Oliveira; Stephen Wallace
Subject: [EXTERNAL EMAIL] - Fwd: NDAO Case Update - SJC ANNOUNCES NEW RULE FOR CELL TOWER DUMPS
Date: Friday, April 1, 2022 4:59:44 PM
Attachments: CW v. Perry - CSLI Tower Dumps April 1 2022.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.

This is our case we worked on.

Sent from my iPhone

Begin forwarded message:

> **From:** "Michael J. D'Entremont" <mdentremont@police.dedham-ma.gov>
> **Date:** April 1, 2022 at 3:35:02 PM EDT
> **To:** "Michael D. Buckley" <mbuckley@police.dedham-ma.gov>, "William D. James" <wjames@police.dedham-ma.gov>, "Bobby Nedder Jr." <bnedder@police.dedham-ma.gov>, "Francis X. McMillan" <fmcmillan@police.dedham-ma.gov>, "John J. Connolly" <jconnolly@police.dedham-ma.gov>, "Keith J. Boyle" <kboyle@police.dedham-ma.gov>, "Jason P. Sullivan" <jsullivan@police.dedham-ma.gov>, "Kevin O. Concannon" <kconcannon@police.dedham-ma.gov>, Michael Doyle <mdoyle@police.dedham-ma.gov>, "Michael Feeley, Jr." <mfeeleyjr@police.dedham-ma.gov>, "Michael R. Feeley" <mfeeley@police.dedham-ma.gov>, "Richard T. Keane" <rkeane@police.dedham-ma.gov>, "Steven L. Munchbach" <smunchbach@police.dedham-ma.gov>, "Timothy J. Chaffee" <tjchaffee@police.dedham-ma.gov>, "Brian R. Cullinane" <brcullinane@police.dedham-ma.gov>, "Brian T. Crump" <bcrump@police.dedham-ma.gov>, Collin O'Sullivan <cosullivan@police.dedham-ma.gov>, "Daniel C. Sullivan" <DSullivan@police.dedham-ma.gov>, Daniel Ford <dford@police.dedham-ma.gov>, "David G. Chambers" <dchambers@police.dedham-ma.gov>, "David M. Connolly" <dconnolly@police.dedham-ma.gov>, "Deborah L. Gonski" <dgonski@police.dedham-ma.gov>, Gregory McCarthy <GMcCarthy@police.dedham-ma.gov>, "James C. Nikolaides" <jnikolaides@police.dedham-ma.gov>, "James J. Quigley" <JQuigley@police.dedham-ma.gov>, "James P. Driscoll" <jdriscoll@police.dedham-ma.gov>, "James T. Lemanski" <jtlemanski@police.dedham-ma.gov>, "John E. Rinn" <jrinn@police.dedham-ma.gov>, "John M. Barrett" <jmbarrett@police.dedham-ma.gov>, John Nolan <jnolan@police.dedham-ma.gov>, Joseph Frasca <jfrasca@police.dedham-ma.gov>, "Joseph K. Ellis" <jellis@police.dedham-ma.gov>, Jtwomey <Jtwomey@police.dedham-ma.gov>, "Ken J. Ellis" <kjellis@police.dedham-ma.gov>, Kevin Mahoney <KMahoney@police.dedham-ma.gov>, "Marissa M. Holland" <mholland@police.dedham-ma.gov>, "Matthew E. Blake" <meblake@police.dedham-ma.gov>, "Matthew S. Kozak"

<mkozak@police.dedham-ma.gov>, Meghan Jenkins <mjenkins@police.dedham-ma.gov>, "Michael R. Pucci" <mpucci@police.dedham-ma.gov>, michael Rahilly <mrahilly@police.dedham-ma.gov>, "Michael W. Power" <mpower@police.dedham-ma.gov>, "Neil F. Cronin" <ncronin@police.dedham-ma.gov>, "Paul M. Cady" <pcady@police.dedham-ma.gov>, Richard Flint <rflint@police.dedham-ma.gov>, "Richard P. Cawley" <rcawley@police.dedham-ma.gov>, Richard Porro <rporro@police.dedham-ma.gov>, Ronald Pucci <rpucci@police.dedham-ma.gov>, "Ryan N. McCarthy" <rnmccarthy@police.dedham-ma.gov>, "Samantha A. Colarusso" <scolarusso@police.dedham-ma.gov>, "Scott D. Porro" <sporro@police.dedham-ma.gov>, "Scott W. Peterson" <speterson@police.dedham-ma.gov>, "Steven J. Feeley" <SFeeley@police.dedham-ma.gov>, "William E. Wilds" <wwilds@police.dedham-ma.gov>

Subject: FW: NDAO Case Update - SJC ANNOUNCES NEW RULE FOR CELL TOWER DUMPS

Michael d'Entremont
Chief of Police
Dedham Police Department
600 High Street
Dedham, MA 02026
781 751-9304
Fax 781 751-9310

From: McLaughlin, Laura A (DAA) <laura.a.mclaughlin@state.ma.us>
Sent: Friday, April 1, 2022 12:29 PM
To: O'Neill, Russ <roneill@brooklinema.gov>; Berkowitz, Kenneth <kberkowitz@town.canton.ma.us>; Quigley, William <wquigley@cohassetpolice.com>; Lennon, Gregory <glennon@cohassetpolice.com>; Michael J. D'Entremont <mdentremont@police.dedham-ma.gov>; McGowan, Peter <pamcgowan@dovermapd.com>; Grace, Michael <mgrace@foxboroughpolice.com>; Michael Collins <mcollins@mpdmilton.org>; Brooks, William G. III <wbrooks@norwoodma.gov>; Keenan, Paul <pkeenan@quincyma.gov>; Anthony Marag <anthonymarag@randolphmapolice.com>; Brewer, Don <dbrewer@townofsharon.org>; Bishop, Kevin <kbishop@townofsharon.org>; Donna McNamara <dmcnamara@stoughton-ma.gov>; jpilecki <jpilecki@wellesleyma.gov>; John Perchard <jperchard@weymouth.ma.us>; Forsythe, Robert (ENV) <robert.forsythe@state.ma.us>; Antoine, Romere (POL) <romere.antoine2@state.ma.us>; Michael Collins <mcollins@mpdmilton.org>; Dicicco, David M (POL) <david.m.dicicco@state.ma.us>; Bukhenik, Yuriy (POL) <yuriy.bukhenik@state.ma.us>; Richard Kelleher <rkelleher@walpolepd.com>; Tully, Brian P (DAA) <brian.p.tully2@state.ma.us>; 'jbukunt@avon-ma.gov' <jbukunt@avon-ma.gov>; 'mdubois@braintreema.gov' <mdubois@braintreema.gov>;

'slydon@braintreema.gov' <slydon@braintreema.gov>; 'mmorgan@brooklinema.gov' <mmorgan@brooklinema.gov>; 'tlynch@franklinpolice.com' <tlynch@franklinpolice.com>; 'wsmith@holbrookpolice.com' <wsmith@holbrookpolice.com>; 'mguerette@medfield.net' <mguerette@medfield.net>; 'amtingley@medwaypolice.com' <amtingley@medwaypolice.com>; 'mreardon@medwaypolice.com' <mreardon@medwaypolice.com>; 'wkingsbury@medwaypolice.com' <wkingsbury@medwaypolice.com>; 'csoffayer@millis.net' <csoffayer@millis.net>; 'jking@mpdmilton.org' <jking@mpdmilton.org>; 'jschlittler@needhamma.gov' <jschlittler@needhamma.gov>; 'cstone@norfolk.ma.us' <cstone@norfolk.ma.us>; 'pkelly@norwoodma.gov' <pkelly@norwoodma.gov>; 'jfloyd@police.plainville.ma.us' <jfloyd@police.plainville.ma.us>; 'williampace@randolphmapolice.com' <williampace@randolphmapolice.com>; 'Melissagreener@randolphmapolice.com' <Melissagreener@randolphmapolice.com>; 'jford@townofsharon.org' <jford@townofsharon.org>; 'jpenders@townofsharon.org' <jpenders@townofsharon.org>; 'pmclaughlin@wellesleyma.gov' <pmclaughlin@wellesleyma.gov>; 'jsilva@westwoodpd.org' <jsilva@westwoodpd.org>; 'rfuller@weymouth.ma.us' <rfuller@weymouth.ma.us>; 'chief@police.wrentham.ma.us' <chief@police.wrentham.ma.us>; 'dbarber@stoughton-ma.gov' <dbarber@stoughton-ma.gov>; 'MMorgan@brooklinema.gov' <MMorgan@brooklinema.gov>; NFK-DL-CPAC <NFK-DL-CPAC@MassMail.State.MA.US>
Cc: Morrissey, Michael W (DAA) <michael.w.morrissey@state.ma.us>; NFK-DL-ADA-Superior-ct <NFK-DL-ADA-Superior-ct@MassMail.State.MA.US>; NFK-DL-ADA-Superior-ct <NFK-DL-ADA-Superior-ct@MassMail.State.MA.US>
Subject: NDAO Case Update - SJC ANNOUNCES NEW RULE FOR CELL TOWER DUMPS

Good afternoon:

Today, April 1, 2022 the Supreme Judicial Court issued a decision in Commonwealth v. Perry that discusses CSLI, tower dumps, and the particularity required in a search warrant affidavit. This case should be read by all prosecutors and officers who draft warrants or rely on cell site information. The case provides an explanation on CSLI (p. 4-8) and the Court's approach to determining whether a search occurred under the "mosaic theory" (p. 13-26).

Facts: Police obtained search warrants for 7 cellphone tower dumps, corresponding to the location of six robberies and an attempted robbery that resulted in a homicide over six dates in 2018 (Sept 22, Sept 27, Sept 28, Oct 4, Oct 6, Oct 25 and Oct 31). The robberies occurred in Boston, Canton and Cambridge. Because each of the robberies was perpetrated in a comparable manner by a man fitting a similar description, police suspected the same person was responsible for all seven incidents. Based on surveillance video and witness statements, police also believed the perpetrator was assisted by a coverturer who acted as the getaway driver.

Police sought search warrants to cross-reference the tower dumps to determine if any device had been near the scene of two or more incidents. After analyzing the information police discovered that a particular telephone number appeared near the scene of two robberies. Police determined, by searching a police database, that this number belonged to the defendant. The defendant was charged with committing all seven robberies and the homicide.

Search Warrants: The Court concluded that the seven town dumps were an intrusion of the defendant's reasonable expectation of privacy and constituted a search, triggering the need for a warrant.

1st warrant: On October 26, 2018 a FBI agent obtained a search warrant from a Federal magistrate judge for tower dumps corresponding to the robberies in Boston, Canton, and Cambridge on September 22, September 27, September 28, and October 4, 2018.

2nd warrant: On January 30, 2019 a Boston police detective obtained a search warrant from a BMC judge for tower dumps corresponding to the October 6, October 25, and October 31 robberies/homicide. This second warrant did not reference or otherwise rely upon evidence obtained from the execution of first warrant.

Both warrants sought the same categories of information. For each cellular telephone that connected to the relevant cell site, the providers were required to furnish (1) the location and sector of the cell site providing service; (2) the telephone number and unique identifier, either of which could be used to identify the owner of the telephone; (3) the type of communication initiated or received when the connection occurred; (4) the telephone number of the device initiating the communication (known as the "source number"); (5) the telephone number of the device receiving the communication (the "destination number"); and (6) the date, time, and duration of each communication.

The execution of the warrants produced information on over 50,000 telephone numbers.

The court found that the 1st warrant did not set-forth particularized information that the perpetrator or the coverturer owned a cellular telephone or communicated with one another from a distance and suppressed all evidence from those tower dumps. In comparison, the 2nd warrant contained particularized information and was upheld.

The differences in the warrants highlight the importance of careful drafting and precise language in a search warrant affidavit.

The **2nd warrant** described several notable similarities between the offenses. Each robbery was committed against a clerk at a store, almost always a convenience store, in or around Boston, sometime during the period between dusk and dark. The perpetrator always brandished a black semiautomatic pistol, which he held in his right hand. Witnesses consistently described the perpetrator as a light-skinned Black or Hispanic male, approximately six feet, two inches tall, with

a medium to thin build, dressed in a black hooded jacket, dark-colored pants, black gloves, black shoes, and a black or red mask. In addition, on two occasions, surveillance footage showed a hole or a light-colored blemish on the robber's jacket. Collectively, this evidence provided a substantial basis to believe, that the same individual had committed all of the offense.
The 2nd warrant also described evidence that a coventurer had acted as a getaway driver in at least three of the offenses. The robberies took place from two to eleven miles apart, and some of the locations were not near any public transportation. On October 4 the store clerk saw the perpetrator enter the passenger's side of a dark-colored sedan, without removing his mask, before quickly departing the scene. On October 6 a surveillance camera captured a dark colored sedan traveling at a high rate of speed along the perpetrator's path of flight. On October 31st police canines detected the perpetrator's scent along his reported flight path, but the scent ended abruptly in a public area with no nearby public transportation, which could have indicated that the perpetrator entered a vehicle. The affidavit also described facts suggesting some reason to believe the defendant and coventurer had communicated with one another from a distance, either prior to or after the commission of the offense. The detective seeking the search warrant averred that, based on his experience and training, violent crimes such as those at issue often require some level of coordination amongst coventurers.

The Court found that because there was reason to believe that the perpetrator used a cellular telephone to communicate with a coventurer around the time of the offenses, there also was probable cause to believe that either the perpetrator's telephone or the coventurer's telephone would have produced telephone call CSLI that would appear in the requested tower dumps, and likely in more than one of the tower dumps. This CSLI, in turn, would enable investigators to isolate potential suspects by determining which, if any, individuals had been near the scene of two or more of the offenses. The affidavit also explained that investigators sought to obtain the tower dumps in order "to identify and/or verify commonalities within [the] requested records." Where the warrant authorized the search of only a narrow subset of CSLI, for purposes of identifying a common suspect, it was sufficiently particular.

In comparison, the **1st warrant** did not discuss the need for coventurers to communicate when committing a robbery, nor did it point to any evidence that the perpetrator and the coventurer had been separated during the commission of the crime such that they would have had to communicate from a distance. The only ground in the first affidavit to conclude that the perpetrator had possessed or used a cellular telephone to aid in accomplishing the crimes was the affiant statement that "it is very common for a person to have a cellular telephone with them at all times." Without more, this was insufficient evidence and the evidence was suppressed.

The Court noted: When seeking a warrant to search CSLI, investigators need not establish that the defendant actually used or possessed his [or her] cell phone during the commission of the crimes, which they would be required to do in order to search its contents. Rather, the nexus requirement is satisfied as long as there is

a substantial basis to conclude that the defendant used his or her cellular telephone during the relevant time frame, such that there is probable cause to believe the sought after CSLI will produce evidence of the crime.

The Court also noted that limiting a search to an identified suspect is best practice where possible, **it is not required where the suspect's identity is unknown and the scope of the search is appropriately limited through other means**.

The SJC used this case to announce the following new rules.

NEW RULES FOR TOWER DUMPS: Before acquiring and analyzing a series of tower dumps, the Commonwealth must obtain a warrant from a judge. Only a judge may issue a search warrant for tower dumps. The warrant must also include protocols for the prompt and permanent disposal of any and all data that does not fit within the object of the search following the conclusion of the prosecution.

Please let me know if you have any questions.

If your department intends to apply for a warrant to search CSLI, tower dumps, or the contents of a cell phone, please don't hesitate to send your search warrant affidavits to my attention for review prior to submitting to the court.

Kindest Regards,

Laura A. McLaughlin
Assistant District Attorney
Norfolk District Attorney's Office
45 Shawmut Road
Canton, MA 02021
(781) 830 – 4800 x 6142
Laura.A.McLaughlin@state.ma.us

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: Paul Allen
To: Manning, David (POL)
Subject: Airship Price Book
Date: Tuesday, August 16, 2022 9:57:26 AM
Attachments: Airship_Price Catalog_2022-2023.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.

Dave, quotes to be shortly forthcoming for [redacted] camera system, with an option for gold and platinum support (0800-2000 vs 24/7/365). Will also include install, configuration, setup and training for administrators and users.

Also attached is our price book which explains the architecture and components. We have talked about Outpost and Outpost Mobile which we will demo tomorrow and have information around included. Once I know what the level of interest is there we can add those to the quote quickly.

Finally, we're waiting today on hardware quotes from Dell, but will have something for you by EOD today that will be for just the recording and management hardware that would sit on top of your existing storage since you have close to 1PB already.

Let me know what else we need, otherwise look forward to tomorrow.

v/r

Paul

The information contained in this transmission is confidential and/or may contain client privileged communications intended for the use of the individual or entity named above, and JDL Digital Systems (DBA Airship Industries, Inc.). If the reader of this electronic message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying is strictly prohibited.

From: Connor, Debora (POL)
To: McCarthy, Steven (POL); Egnitz, Brian (POL)
Cc: Connor, Debora (POL)
Subject: ALPR and 4RE Email
Date: Monday, February 28, 2022 11:10:47 AM
Attachments: APLR and 4RE decision.msg

FYI

Debora Connor
Special Projects Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-861-6743

The information transmitted is intended only for the person or entity to which 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: Breck, Kathy
To: Pack, Noah (POL)
Cc: Martucci, J
Subject: ALPR TENANT MOU, with SPD proposed edits
Date: Tuesday, April 26, 2022 12:49:41 PM
Attachments: ALPR TENANT MOU, with SPD proposed edits.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.

Dear Sgt. Pack/Noah:

Attached is the Mass. State Police ALPR MOU with my comments and proposed redlined changes in sections 4 and 11, on behalf of the Springfield Police Dept. Thank you for forwarding for MSP legal review.

Best regards,
Kathy Breck 4/26/22

Kathleen T. Breck
Deputy City Solicitor
City of Springfield Law Department
36 Court Street, Room 210
Springfield, MA. 01103
(413)787-6179
kbreck@springfieldcityhall.com

From: Keeler, Dennis (POL)
To: Grassia, Michael (POL); Michael Grassia; Arredondo, Elkin (POL); O"Brien, Mark (POL); Traister, Michael (POL); Haines, Michael (POL); Hartley, Daniel (POL)
Subject: Automated License Plate Reader (ALPR) training notes
Date: Wednesday, May 25, 2022 12:24:36 PM
Attachments: TRF-11 Automatic License Plate Recognition.pdf

Good morning,

Some notes about this morning's training from Sgt Noah Pack regarding the ALPR training. I'm sure you guys know more about this than I do but the training was definitely useful and well done.

MSP is looking to train all supervisors on this software and issued username / password to us for administrative purposes. Many of these formal requests can be done through the MSP Watch Center as we have in the past. Legal process (search warrant / GJ subpoena) may be needed if we are intend on using ALPR data in a court case.

Comm vs. McCarthy (2020) is the legal precedent essentially stating LE may use data points from ALPR for "limited circumstances". This was a Cape Cod narcotics case that used the Cape bridges ALPRs. It outlined that too much data retrieval, too broad geographical search or too vague a timeline can be construed as a search and therefore will be inadmissible.

Legal process for ALPR data should be obtained through a court-issued SW that then gets forwarded to EOPSS then to DOT. Strange, circuitous route but that's what Noah said. EOPSS is currently blocking the use of MSP cruiser-mounted cameras. In exigent circumstances, ALPR usage is widely acceptable. For investigative means, ALPR analysis should be case specific and time / geographical location sensitive. Apparently, the MA courts are really paying attention to these factors. ACLU is giving their standard pushback on the system as a whole.

[redacted] [ALPR link]
Username: [redacted]
PW: [redacted]

Note: Send me a quick email when/if you access the ALPR system with the above username & password. The onus of the specific searches are on the supervisors; we are trying to avoid negative case law that brings additional scrutiny on this useful LE tool.

As far as the ALPR (Neology / Boss 4) website goes, it's web-based and cloud-accessible so it will not have the MSP firewall. You can access it from anywhere. The ALPR is guided by MSP policy TRF-11 [attached]. The above user name and password is for our immediate unit only. If we are putting a case together where we are using ALPR often, we have the ability to add TFO & local officer access. Any outside agency looking for assistance, help them manually or refer them to the MSP Watch Center where they'll track and log all assistance on ACISS. Makes our lives

easier.

When you log on, you'll see 3 options on the main menu bar: (1) analytics (2) reads (3) system. Each has a drop down list and filtering abilities. If you want to practice, use your GSA vehicle plate. The options you should be most familiar with are:

"Reads" --> Search [justification, license plate, time frame, etc]
"Reads" --> Report [ordered report on suspect plate(s)/MV/etc]
"System" --> Hotlists [MVs you want on hotlist]
"System" --> Notifications [alert on suspect MVs]

The navigation within these options is relatively self-explanatory. You can type in case notes, case #, etc to stoke your memory if juggling multiple cases. The reports are kept for approximately 90 days.

When searching for a vehicle, play around with the filter option on the left, specifically "Mantis Vehicle ID". This options allows you to get more specific if the plate is unknown but the vehicle description and/or date & time is known. The "Device" filter allows you to navigate by location which may satisfy the courts specificity issues should the data become evidence.

The reports can be exported in an Adobe PDF form and/or Excel if applicable. Again, I'm sure much of this is old hat to you guys but give me a buzz with any questions.

Respectfully,

Sergeant Dennis D. Keeler #3132
Massachusetts State Police
SIU/FBI Violent Crimes Task Force
[C] [redacted]

From: Miller, Dianne (POL)
To: Kearnan, Brian J. (POL)
Subject: Axon > Summary of exceptions to conditions
Date: Monday, March 7, 2022 12:18:00 PM
Attachments: Summary of exceptions to conditions.docx
Exceptions and MSPA_Axon.pdf
image001.png

Hi
I put together a summary of Axon's exceptions to the RFR and Commonwealth conditions, please see attached.
My draft email to Eric @ Axon is to clarify a few of the exceptions.

Thanks

Dianne Miller
Massachusetts State Police
Program Coordinator III
470 Worcester Road
Framingham, MA 01702
508-820-2143

To: Eric Sorlie
Cc: Kearnan, Brian J. (POL)
Subject: Axon Clarifications of Terms and Conditions
Date: Monday, March 7, 2022 4:46:12 PM
Attachments: image001.png
Exceptions and MSPA_Axon.pdf
Axon Pricing and Products - FINAL.xlsb
Terms and Conditions.pdf
RFR_SP22-AMMO-X86.doc

Good afternoon Eric,

I have a couple of questions (in red font) regarding the attached Axon "Exceptions and MSPA" document:

1. RFR Section 1.6. Anticipated Expenditures, Funding or Compensation:
Axon requests the following modifications. Pricing for five and ten year programs will be held firm for the term specified on the quote; however, we request the opportunity to adjust pricing changes during the 3 year term of the contract where justified.

[…] Contract Quoted prices will remain fixed during the ~~initial contract period~~ entire term of the quote. Contractors will have an opportunity to request a price increase if an option to renew is offered on a yearly basis. Contractors will need to submit written justification and supporting documentation with price increase requests. The Department of State Police does not guarantee that increase requests will be granted

MSP: Where are the five and ten year programs presented in the Axon bid response?
MSP: The attached FINAL pricing document does not specify how long the prices are held firm. The contract initial duration is 3 years.
MSP can be flexible regarding price increases during the initial 3 year contract duration, with justification.

2. RFR Section 2.2.9. Order Cancellation. Axon requests that this be clarified to specify that order cancellation will be limited to orders which have not been shipped. Once shipped, an individual order may be terminated in accordance with the termination procedure laid out in the contract.

MSP: which termination procedure are you referring to? TASER7 agreement?

3. Section 4.1. Contractor Terms. Axon respectfully requests that its TASER 7 Agreement, which contains terms specific to the licensing and subscription models and financing program associated with the hardware and software being offered in response to this solicitation, be incorporated as an exhibit into the final contract award. Axon agrees to negotiate these terms and conditions in good faith, and in the event of any conflict with the Commonwealth Terms and Conditions, the Commonwealth's terms and conditions will control.

MSP: Under review. Typically an agreement such as this would be incorporated into the actual purchase and attached to the Axon quote.
The contract award is to put bidders on a qualified list of contractors, the quote/purchase order is processed at a future date.

Regarding items 4, 5, and 6 from the Commonwealth Terms and Conditions:

The Commonwealth Terms and Conditions are jointly issued by the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) for use by all Commonwealth of Massachusetts ("State") Departments and Contractors.
As its issued by three separate parent agencies with procurement oversight, we are simply unable to modify it.

Dianne Miller
Massachusetts State Police
Program Coordinator III
470 Worcester Road
Framingham, MA 01702
508-820-2143

To: Eric Sorlie
Cc: Kearnan, Brian J. (POL)
Subject: Axon Clarifications of Terms and Conditions
Date: Monday, March 7, 2022 11:33:33 AM
Attachments: image001.png
Exceptions and MSPA_Axon.pdf

Good morning Eric,

I'll review the attached exceptions with my manager Brian Kearnan and if needed, our legal staff.

I have a couple of questions first:

The Commonwealth Terms and Conditions are jointly issued by the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) for use by all Commonwealth of Massachusetts ("State") Departments and Contractors. As its issued by three separate parent agencies with procurement oversight, we are simply unable to modify it.

Dianne Miller
Massachusetts State Police
Program Coordinator III
470 Worcester Road
Framingham, MA 01702
508-820-2143

From: Miller, Dianne (POL)
To: Eric Sorlie
Cc: Kearnan, Brian J. (POL)
Subject: Axon Clarifications of Terms and Conditions
Date: Monday, March 7, 2022 4:49:00 PM
Attachments: image001.png
Exceptions and MSPA_Axon.pdf
Axon Pricing and Products - FINAL.xlsb
Terms and Conditions.pdf
RFR_SP22-AMMO-X86.doc

Good afternoon Eric,

I have a couple of questions (in red font) regarding the attached Axon "Exceptions and MSPA" document:

1. RFR Section 1.6. Anticipated Expenditures, Funding or Compensation:
Axon requests the following modifications. Pricing for five and ten year programs will be held firm for the term specified on the quote; however, we request the opportunity to adjust pricing changes during the 3 year term of the contract where justified.

[…] Contract Quoted prices will remain fixed during the ~~initial contract period~~ entire term of the quote. Contractors will have an opportunity to request a price increase if an option to renew is offered on a yearly basis. Contractors will need to submit written justification and supporting documentation with price increase requests. The Department of State Police does not guarantee that increase requests will be granted

MSP: Where are the five and ten year programs presented in the Axon bid response?
MSP: The attached FINAL pricing document does not specify how long the prices are held firm. The contract initial duration is 3 years.
MSP can be flexible regarding price increases during the initial 3 year contract duration, with justification.

2. RFR Section 2.2.9. Order Cancellation. Axon requests that this be clarified to specify that order cancellation will be limited to orders which have not been shipped. Once shipped, an individual order may be terminated in accordance with the termination procedure laid out in the contract.

MSP: which termination procedure are you referring to? Section 13 of the TASER7 agreement?

3. Section 4.1. Contractor Terms. Axon respectfully requests that its TASER 7 Agreement, which contains terms specific to the licensing and subscription models and financing program associated with the hardware and software being offered in response to this solicitation, be incorporated as an exhibit into the final contract award. Axon agrees to negotiate these terms and conditions in good faith, and in the event of any conflict with the Commonwealth Terms and Conditions, the Commonwealth's terms and conditions will control.

MSP: Under review. Typically an agreement such as this would be incorporated into the actual purchase and attached to the Axon quote.
The contract award is to put bidders on a qualified list of contractors, the quote/purchase order is processed at a future date.

Regarding items 4, 5, and 6 from the Commonwealth Terms and Conditions:

The Commonwealth Terms and Conditions are jointly issued by the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) for use by all Commonwealth of Massachusetts ("State") Departments and Contractors.
As its issued by three separate parent agencies with procurement oversight, we are simply unable to modify it.

Dianne Miller
Massachusetts State Police
Program Coordinator III
470 Worcester Road
Framingham, MA 01702
508-820-2143

From: John Tedona
To: Pack, Noah (POL)
Subject: Bergen County NJ ALPR Policy
Date: Friday, August 12, 2022 9:34:55 AM
Attachments: image001.png
image002.png
image003.png
Marty Delaney.ppt
AG Guidelines Final.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,

Following up on our conversation the other day I attached a dated, but still relevant, ALPR guidelines that Bergen County instituted during the time when ALPR technology first began getting traction in law enforcement. This was a PowerPoint that was presented to all 70 local agencies that were connected to BOSS. He used to present before me in all training session to the local agencies to ensure they all utilized ALPR per the County guidelines. Marty Delaney had retired in 2020.

I'm not sure if the attached ALPR AG Guideline is the current version, but NJ is expected to releases the latest policy within the next few weeks.

I'm still waiting for the NJSP ALPR coordinator to okay that I give you his name to contact. NJSP is very secretive, but I don't he'll have any problem speaking with you.

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: Cormier, Donald (POL)
To: Pack, Noah (POL)
Subject: CJIS Agreement
Date: Friday, March 4, 2022 12:19:37 PM
Attachments: SP Framingham GHQ 01-12-2021.pdf
Global Justice Public Safety Agreement FINAL 9-28-2020.docx

Noah,

Is this what you were looking for?

Captain Donald J. Cormier #812
Massachusetts State Police
Division of Administrative Services
470 Worcester Rd.
Framingham, MA. 01702
(508) 820-2107
Email:donald.cormier@massmail.state.ma.us

From: Sarasin, Ryan (CHS) <ryan.sarasin@mass.gov>
Sent: Friday, March 4, 2022 10:25 AM
To: Cormier, Donald (POL) <donald.cormier@pol.state.ma.us>
Subject: RE: CJIS Agreement

Captain,

Attached is a copy of your most recent user agreement (not the global sharing agreement), but just your user agreement for CJIS.

That Global Sharing Agreement document that was attached is typically for the license plate readers, COPLINK, and a few others. I looked and it does not look like we have one of these on file for MSP. I am going to inquiry about whether we should moving forward, but right now it doesn't look like we do. I also attached a more recent Global Sharing Agreement that goes into a little more detail about the scope and need for the document.

Do you know what vendor (name) is asking for this document and the exact purpose. I understand they want to make sure you are authorized to access CJIS data. In my opinion, the user agreement does show you have the authority, I just want to confirm the vendor.

Thanks Captain!

-Ryan

From: Hutchinson, Daniel (CHS)
To: Hutchinson, Daniel (CHS)
Subject: CJIS REP Training
Date: Thursday, October 13, 2022 11:24:56 AM
Attachments: CJIS-REP GUIDE .doc

Good Morning,

I've attached a CJIS REP Guide for use during the training scheduled on Thursday, October 27th, 2022, 9:00a.m., at the MPTC located at 42 Thomas Petten Dr., Randolph, MA 02358. Please make a copy of the guide and bring it with you to the training. The CJIS Support Services Unit is looking forward to meeting everyone and providing this training. If you have any specific issues relating to CJIS that you have encountered and would like discussed send me a separate email so that I can research the issue prior to the training.

Thank you,

Dan Hutchinson

Daniel J. Hutchinson
Massachusetts Department of Criminal Justice Information Services
CJIS Support Services
200 Arlington Street-Suite 2200
Chelsea, MA 02150
F: 617-884-4601
Daniel.Hutchinson@mass.gov | www.mass.gov/cjis

To: Halpin, Michael (POL)
Subject: coastal cameral policy
Date: Monday, October 31, 2022 4:44:45 PM
Attachments: image001.png

In this case, as in McCarthy, we are considering the import of a relatively small number of cameras, here, five. Only two of these cameras were targeted at Mora's and Suarez's residences. *369 The defendants nonetheless argue that all footage from any of the five cameras that captures their comings and goings must be suppressed under the mosaic theory. We do not agree. Rather, we conclude that the cameras installed to surveil the defendants' homes were of greater constitutional significance than those, as in McCarthy, that were directed at a public highway.
13141516A. Surveillance away from the defendants' home. To the extent that the pole cameras in this case surveilled the defendants away from their own homes, we conclude that this surveillance, like the ALPR use in McCarthy, was not a search in the constitutional sense. At most, it appears that Mora, Suarez, and Guerrero were each captured, on a few occasions, by two cameras directed at a different codefendant's residence. Such short-term, intermittent, and nontargeted video recording of a person away from his or her own home is little different from being captured by the security cameras that proliferate in public spaces. The United States Supreme Court recognized this traditional nontargeted use of video cameras when it referred to "security cameras" as among the "conventional surveillance techniques and tools" that were not called into question by its holding in Carpenter, 138 S. Ct. at 2220. Law enforcement officers appropriately have relied on security cameras, and other forms of nontargeted video surveillance, to identify and apprehend suspects, particularly in emergency **308 situations.[10] See, e.g., United States v. Tsarnaev, 53 F. Supp. 3d 450, 458 (D. Mass. 2014) (describing evidence obtained from privately-owned surveillance camera in investigation of Boston Marathon bombing). *370 See also Commonwealth v. Leiva, 484 Mass. 766, 770 & n.5, 146 N.E.3d 1093 (2020); Commonwealth v. Ferreira, 481 Mass. 641, 645, 119 N.E.3d 278 (2019); Commonwealth v. Boswell, 374 Mass. 263, 265-267, 372 N.E.2d 237 (1978).
17In the circumstances here, the limited pole camera surveillance of Mora and Suarez away from their homes did not collect aggregate data about the defendants over an extended period. Without such data, the cameras similarly did not allow investigators to generate a mosaic of the defendants' private lives that otherwise would have been unknowable. Cf. McCarthy, 484 Mass. at 502, 142 N.E.3d 1090. Therefore, as we held in McCarthy, this limited surveillance falls within the general rule that a person has no reasonable expectation of privacy in what he or she knowingly exposes to the public.

Commonwealth v. Mora, 150 N.E.3d 297, 307–08, 485 Mass. 360, 368–70 (Mass., 2020)

Whether Zachery's expectation of privacy is one that society is prepared to recognize is a more difficult question. We have recognized that "a privacy interest in the whole of one's public movements" exists. McCarthy, 484 Mass. at 502, 142 N.E.3d 1090.
See Riley v. California, 573 U.S. 373, 403, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). This privacy interest can be implicated continually, as when the government affixes a location-tracking device to a suspect's vehicle. See Commonwealth v. Rousseau, 465 Mass. 372, 382, 990 N.E.2d 543 (2013). See also Jones, 565 U.S. at 404, 132 S.Ct. 945. Under the mosaic theory, it also can be implicated as a result of data aggregation.
See McCarthy, supra at 503, 142 N.E.3d 1090. Indeed, "[w]hen collected for a long enough

period, 'the cumulative nature of the information collected implicates a privacy interest on the part of the individual who is the target of the tracking.' " Id., quoting Augustine, 467 Mass. at 253, 4 N.E.3d 846. See *110 Mora, 485 Mass. at 373, 150 N.E.3d 297 ("our analysis under art. 14 turns on whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life"). 2223"The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps." See Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012). Under the mosaic theory, while each individual piece of information collected may not amount to a search, the cumulative, aggregate nature of the data collected may. See id.
In McCarthy, 484 Mass. at 506, 142 N.E.3d 1090, we adopted the mosaic theory in the context of automatic license plate reader cameras. Although we held that four cameras located at the ends of two bridges did not reveal information that rose to the level of a search, we acknowledged that "[a] detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts." Id. at 504, 142 N.E.3d 1090. Here, Zachery argues that the mosaic theory applies to the cumulative nature of **1105 the information collected from his CharlieCard. While we agree that an extensive record of an individual's MBTA activity could constitute a search under the mosaic theory, the minimal amount of data obtained in this case does not constitute a violation of art. 14 or the Fourth Amendment. Whether the aggregation of data collected by police implicates the mosaic theory depends on how much data police retrieved and the time period involved. See Mora, 485 Mass. at 370, 150 N.E.3d 297. See also Commonwealth v. Estabrook, 472 Mass. 852, 858, 38 N.E.3d 231 (2015). The MBTA has the ability to retain fourteen months of an individual's travel history through the individual's CharlieCard. There is no question that such extensive data, in certain circumstances, could create a "highly detailed profile." Commonwealth v. Connolly, 454 Mass. 808, 834, 913 N.E.2d 356 (2009) (Gants, J., concurring), quoting People v. Weaver, 12 N.Y.3d 433, 442, 882 N.Y.S.2d 357, 909 N.E.2d 1195 (2009). From this information, MBTA police also can search for and retrieve video footage.

Commonwealth v. Henley, 171 N.E.3d 1085, 1104–05, 488 Mass. 95, 109–10 (Mass., 2021)

9Here the pole camera, which was placed across the street from the defendant's residence, captured footage of the residence's exterior, including the front entrance, the left side of the building, and the driveway over the course of approximately fifteen days.[9] "[T]argeted long-term pole camera surveillance of the area surrounding a residence has the capacity to invade the security of the home," as it "captures ... revealing interactions at the threshold of a person's private and public life." Mora, 485 Mass. at 371, 373, 150 N.E.3d 297.
The camera allowed investigators either to monitor the defendant in real time as he arrived to and departed from the residence, or to search the footage by date and time. Thus, the investigators had the "ability to 'pick out and identify individual, sensitive moments that would otherwise be lost to the natural passage of time.' " Id. at 375, 150 N.E.3d 297, quoting Levinson-Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public, 66 Emory L.J. 527, 603 (2017). We conclude that under these circumstances the defendant's expectation of privacy was reasonable; thus, the pole camera surveillance constituted a search under art. 14.

Commonwealth v. Comenzo, 180 N.E.3d 453, 458, 489 Mass. 155, 160 (Mass., 2022)

The office was not limited to the plaintiff's exclusive use, and the over-all public exposure of the physical layout abrogated any expectation that her actions, while in the office, would be private. See generally *id.* at 179–180, and cases cited (noting that where the work area in question is not given over to an employee's exclusive use, this factor militates against an objectively reasonable expectation of privacy). Cf. *United States v. Taketa,* 923 F.2d 665, 673 (9th Cir.1991) (finding reasonable expectation of privacy in locked, private office). *536 Although, unlike the plaintiffs in the *Vega–Rodriguez* case, the plaintiff lacked notice of the defendants' surveillance of the office, the facts of this case, including the explicitly public nature of the work conducted by the SBDC and the ready visual and physical access that was afforded the public, all employees (including management) and volunteers by the SBDC, abrogated any objectively reasonable expectation of privacy. See, e.g., *Vega–Rodriguez v. Puerto Rico Tel. Co., supra* at 180 (Fourth Amendment does not preclude "management from observing electronically what it lawfully can see with the naked eye"). We **348 now turn to the remaining issues of the case.

Nelson v. Salem State College, 845 N.E.2d 338, 347–48, 446 Mass. 525, 535–36 (Mass.,2006)

From: Halpin, Michael (POL)
To: Halpin, Michael (POL)
Subject: coastal cameral policy
Date: Monday, October 31, 2022 4:46:00 PM
Attachments: image001.png

In this case, as in McCarthy, we are considering the import of a relatively small number of cameras, here, five. Only two of these cameras were targeted at Mora's and Suarez's residences. *369 The defendants nonetheless argue that all footage from any of the five cameras that captures their comings and goings must be suppressed under the mosaic theory. We do not agree. Rather, we conclude that the cameras installed to surveil the defendants' homes were of greater constitutional significance than those, as in McCarthy, that were directed at a public highway.
13141516A. Surveillance away from the defendants' home. To the extent that the pole cameras in this case surveilled the defendants away from their own homes, we conclude that this surveillance, like the ALPR use in McCarthy, was not a search in the constitutional sense. At most, it appears that Mora, Suarez, and Guerrero were each captured, on a few occasions, by two cameras directed at a different codefendant's residence. Such short-term, intermittent, and nontargeted video recording of a person away from his or her own home is little different from being captured by the security cameras that proliferate in public spaces. The United States Supreme Court recognized this traditional nontargeted use of video cameras when it referred to "security cameras" as among the "conventional surveillance techniques and tools" that were not called into question by its holding in Carpenter, 138 S. Ct. at 2220. Law enforcement officers appropriately have relied on security cameras, and other forms of nontargeted video surveillance, to identify and apprehend suspects, particularly in emergency **308 situations.[10] See, e.g., United States v. Tsarnaev, 53 F. Supp. 3d 450, 458 (D. Mass. 2014) (describing evidence obtained from privately-owned surveillance camera in investigation of Boston Marathon bombing). *370 See also Commonwealth v. Leiva, 484 Mass. 766, 770 & n.5, 146 N.E.3d 1093 (2020); Commonwealth v. Ferreira, 481 Mass. 641, 645, 119 N.E.3d 278 (2019); Commonwealth v. Boswell, 374 Mass. 263, 265-267, 372 N.E.2d 237 (1978).
17In the circumstances here, the limited pole camera surveillance of Mora and Suarez away from their homes did not collect aggregate data about the defendants over an extended period. Without such data, the cameras similarly did not allow investigators to generate a mosaic of the defendants' private lives that otherwise would have been unknowable. Cf. McCarthy, 484 Mass. at 502, 142 N.E.3d 1090. Therefore, as we held in McCarthy, this limited surveillance falls within the general rule that a person has no reasonable expectation of privacy in what he or she knowingly exposes to the public.

Commonwealth v. Mora, 150 N.E.3d 297, 307–08, 485 Mass. 360, 368–70 (Mass., 2020)

Whether Zachery's expectation of privacy is one that society is prepared to recognize is a more difficult question. We have recognized that "a privacy interest in the whole of one's public movements" exists. McCarthy, 484 Mass. at 502, 142 N.E.3d 1090.
See Riley v. California, 573 U.S. 373, 403, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). This privacy interest can be implicated continually, as when the government affixes a location-tracking device to a suspect's vehicle. See Commonwealth v. Rousseau, 465 Mass. 372, 382, 990 N.E.2d 543 (2013). See also Jones, 565 U.S. at 404, 132 S.Ct. 945. Under the mosaic theory, it also can be implicated as a result of data aggregation.

See McCarthy, supra at 503, 142 N.E.3d 1090. Indeed, "[w]hen collected for a long enough period, 'the cumulative nature of the information collected implicates a privacy interest on the part of the individual who is the target of the tracking.' " Id., quoting Augustine, 467 Mass. at 253, 4 N.E.3d 846. See *110 Mora, 485 Mass. at 373, 150 N.E.3d 297 ("our analysis under art. 14 turns on whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life"). 2223"The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps." See Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012). Under the mosaic theory, while each individual piece of information collected may not amount to a search, the cumulative, aggregate nature of the data collected may. See id.
In McCarthy, 484 Mass. at 506, 142 N.E.3d 1090, we adopted the mosaic theory in the context of automatic license plate reader cameras. Although we held that four cameras located at the ends of two bridges did not reveal information that rose to the level of a search, we acknowledged that "[a] detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts." Id. at 504, 142 N.E.3d 1090. Here, Zachery argues that the mosaic theory applies to the cumulative nature of **1105 the information collected from his CharlieCard. While we agree that an extensive record of an individual's MBTA activity could constitute a search under the mosaic theory, the minimal amount of data obtained in this case does not constitute a violation of art. 14 or the Fourth Amendment. Whether the aggregation of data collected by police implicates the mosaic theory depends on how much data police retrieved and the time period involved. See Mora, 485 Mass. at 370, 150 N.E.3d 297. See also Commonwealth v. Estabrook, 472 Mass. 852, 858, 38 N.E.3d 231 (2015). The MBTA has the ability to retain fourteen months of an individual's travel history through the individual's CharlieCard. There is no question that such extensive data, in certain circumstances, could create a "highly detailed profile." Commonwealth v. Connolly, 454 Mass. 808, 834, 913 N.E.2d 356 (2009) (Gants, J., concurring), quoting People v. Weaver, 12 N.Y.3d 433, 442, 882 N.Y.S.2d 357, 909 N.E.2d 1195 (2009). From this information, MBTA police also can search for and retrieve video footage.

Commonwealth v. Henley, 171 N.E.3d 1085, 1104–05, 488 Mass. 95, 109–10 (Mass., 2021)

9Here the pole camera, which was placed across the street from the defendant's residence, captured footage of the residence's exterior, including the front entrance, the left side of the building, and the driveway over the course of approximately fifteen days.[9] "[T]argeted long-term pole camera surveillance of the area surrounding a residence has the capacity to invade the security of the home," as it "captures ... revealing interactions at the threshold of a person's private and public life." Mora, 485 Mass. at 371, 373, 150 N.E.3d 297.
The camera allowed investigators either to monitor the defendant in real time as he arrived to and departed from the residence, or to search the footage by date and time. Thus, the investigators had the "ability to 'pick out and identify individual, sensitive moments that would otherwise be lost to the natural passage of time.' " Id. at 375, 150 N.E.3d 297, quoting Levinson-Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public, 66 Emory L.J. 527, 603 (2017). We conclude that under these circumstances the defendant's expectation of privacy was reasonable; thus, the pole camera surveillance constituted a search under art. 14.

Commonwealth v. Comenzo, 180 N.E.3d 453, 458, 489 Mass. 155, 160 (Mass., 2022)

The office was not limited to the plaintiff's exclusive use, and the over-all public exposure of the physical layout abrogated any expectation that her actions, while in the office, would be private. See generally *id.* at 179–180, and cases cited (noting that where the work area in question is not given over to an employee's exclusive use, this factor militates against an objectively reasonable expectation of privacy). Cf. *United States v. Taketa,* 923 F.2d 665, 673 (9th Cir.1991) (finding reasonable expectation of privacy in locked, private office). *536 Although, unlike the plaintiffs in the *Vega–Rodriguez* case, the plaintiff lacked notice of the defendants' surveillance of the office, the facts of this case, including the explicitly public nature of the work conducted by the SBDC and the ready visual and physical access that was afforded the public, all employees (including management) and volunteers by the SBDC, abrogated any objectively reasonable expectation of privacy. See, e.g., *Vega–Rodriguez v. Puerto Rico Tel. Co., supra* at 180 (Fourth Amendment does not preclude "management from observing electronically what it lawfully can see with the naked eye"). We **348 now turn to the remaining issues of the case.

Nelson v. Salem State College, 845 N.E.2d 338, 347–48, 446 Mass. 525, 535–36 (Mass.,2006)

From: Stone, Jessica (DAA)
To: DAA-DL-DA&EXEC.ASST; DAA-DL-ADA"s; DAA-DL-Case Summaries
Subject: Court Decision - Commonwealth v. Jerron Perry (Cell Towers, Search & Seizure, Expectation of Privacy) - April 1, 2022
Date: Friday, April 1, 2022 11:32:53 AM
Attachments: image001.png
Commonwealth v. Jerron Perry.pdf

Commonwealth v. Jerron Perry
Supreme Judicial Court – April 1, 2022
(Cell Towers, Search & Seizure, Expectation of Privacy)

In a lengthy and detailed decision, the Court addressed the constitutional implications of "tower dumps", which provide the cell site location information (CSLI) for all devices that connect to specific cell towers during a particular time period.

Background: The Commonwealth obtained search warrants for seven tower dumps, corresponding to the locations of six robberies and an attempted robbery which resulted in a homicide. The dumps spanned seven different days over the course of slightly more than one month; each tower dump was limited in time to the period immediately before and after the specific robbery for which the CSLI was sought. Investigators then cross-referenced the information obtained from the tower dumps to isolate particular telephone numbers that appeared at more than one location. Thereafter, investigators analyzed the CSLI associated with those telephone numbers, among them the defendant's telephone number, to "determine (1) the approximate location of the connecting cellular telephone, (2) the identity of the telephone's user, and (3) the identity of the person with whom the user was communicating." In total, police obtained information on over 50,000 distinct phone numbers. By cross referencing the data, police determined that the defendant's number appeared in the tower dump pertaining to the homicide on Oct. 6, 2018 and the robbery on Oct. 31, 2018. Police also learned "that, at around the time of the shooting on October 6, 2018, the defendant's telephone had been in communication with another device, which they suspected to have belonged to the getaway driver. Investigators were able to determine the identity of the suspected coventurer, as well as the fact that his cellular telephone number appeared in the tower dumps corresponding to the robberies on September 22, October 6, and October 31, 2018." The defendant moved to suppress all evidence obtained from the data towers, and when his motion was denied a single justice reserved and reported to the full court.

Holding: "We agree that the government's use of the seven tower dumps was an intrusion upon the defendant's reasonable expectation of privacy, and therefore constituted a search under art. 14 of the Massachusetts Declaration of Rights. We do not agree, however, that warrants for tower dumps are per se unconstitutional. Accordingly, investigators may use tower dumps so long as they comply with the warrant requirements of art. 14."

The Court exercised its powers pursuant to G.L. c. 211 s. 3 and held that going forward, before acquiring and analyzing a series of tower dumps, the "Commonwealth must obtain a warrant from a judge. Before issuing the requested warrant, the judge must ensure that it provides a protocol for the disposal of any data that falls outside the scope of the search." The Court also determined that "our holding applies prospectively and to those cases that are active or pending on direct review on the date of issuance of the rescript in this case."

Application: In determining whether the police use of technology to engage in long-term surveillance "constitute[d] a search under the mosaic theory, courts have considered 'whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life. … To answer this question, our limited precedent to date primarily has focused on three general concerns: the extent to which the surveillance reveals the whole of an individual's public movements; the character of the information obtained; and whether the surveillance could have been achieved using traditional law enforcement techniques. … While these factors have emerged as preeminent in the few cases in which we have applied the mosaic theory to date, we emphasize that the question whether electronic surveillance exposes otherwise unknowable details of a person's life must be answered in light of the totality of the circumstances in each case. Accordingly, these factors are not exhaustive, and no one factor is determinative." The Court found that here, the actions of the police--viewed in their entirety—provided police with information of a "highly personal and private nature" previously "unknowable" about the defendant's life. Therefore, the use of the seven tower dumps intruded upon the defendant's reasonable expectation of privacy.

It was undisputed that the Commonwealth had established probable cause to believe that the crimes described in the warrants had been committed. Therefore, the Court focused its analyses on whether the warrants established a substantial basis to believe that a search of the requested tower dumps would provide evidence of the crimes under investigation, or would aid in the apprehension of the perpetrator.

First Warrant:

Probable Cause: The affidavit did not set forth any particularized information that the perpetrator or the coventurer owned a cell phone or communicated with each other from a distance. "Moreover, the first warrant affidavit did not discuss the need for coventurers to communicate when committing a robbery, nor did it point to any

evidence that the perpetrator and the coventurer had been separated during the commission of the crime such that they would have had to communicate from a distance. Thus, the only ground in the first affidavit upon which to conclude that the perpetrator had possessed or used a cellular telephone to aid in accomplishing the crimes was the affiant officer's statement that "it is very common for a person to have a cellular telephone with them at all times." Therefore, the information from the first warrant "must be" suppressed.

Particularity: Not reached due to the finding of no probable cause.

Second Warrant:

Probable Cause: The Court found that the affidavit described several similarities between the offenses and evidence that a second co-venturer had acted as a getaway driver in at least three of the crimes. IT also contained information suggesting that the defendant and co-venturer had communicated with each other from a distance either before or after the crime. The second warrant did not rely on any data produced from the first warrant. "The evidence that the perpetrator and the coventurer communicated from a distance, when combined with the affiant's statements about the over-all ubiquity of cellular telephones, provided reasonable grounds to believe that the robber and the getaway driver had used cellular telephones to communicate. Because there was reason to believe that the perpetrator used a cellular telephone to communicate with a coventurer around the time of the offenses, there also was probable cause to believe that either the perpetrator's telephone or the coventurer's telephone would have produced telephone call CSLI that would appear in the requested tower dumps, and likely in more than one of the tower dumps. This CSLI, in turn, would enable investigators to isolate potential suspects by determining which, if any, individuals had been near the scene of two or more of the offenses. Accordingly, the second warrant was supported by probable cause."

Particularity: "The defendant's reasonable expectation of privacy was invaded not simply by law enforcement's possession of his anonymized CSLI, but also by the investigating officers' possession and analysis of that CSLI, the aggregate of which provided investigators with a revealing mosaic of the defendant's private life. Only those individuals whose CSLI was subject to further analysis – such as the defendant -- were subject to a search within the meaning of art. 14. The question, then, becomes whether the second warrant sufficiently limited the set of telephone numbers and their associated CSLI that investigating officers were permitted to analyze, and therefore to search." The Court found that while the scope of the warrant and particular items to be seized were not "entirely clear" and could have permitted investigators to "permissibly could select any telephone number from among the 50,000 provided and thereafter conduct a search by determining the identity of that individual, his or her location, and with whom he or she had been communicating, all without even an iota of suspicion", any defects were remedied by the supporting affidavit which adequately limited the scope of the search.

"Otherwise put, because the warrant authorized the search of only a narrow subset of the CSLI, for purposes of identifying a common suspect, it was sufficiently particular."

PRACTICE TIP: "Although limiting a search of CSLI to an identified suspect might be the better practice where possible, it is not required where, as here, the suspect's identity is unknown and the scope of the search is appropriately limited through other means."

NOTE: The Court distinguished this case from its 2015 holding in *Estabrook*-- a warrantless search of up to six continuous hours of CSLI was permissible—on the grounds that here the government obtained small increments of CSLI over the course of different days. "The rationale in *Estabrook* was that analyzing six hours or less of telephone call CSLI could not be a search 'because the duration is too brief to implicate the person's reasonable privacy interest.' While the court has determined that analyzing six continuous hours of CSLI does not intrude upon a reasonable expectation of privacy, analyzing small increments of CSLI over the course of several days does. Accordingly, although *Estabrook* enables the Commonwealth to obtain one or more tower dumps spanning six hours or less without a warrant, it provides no refuge where, as here, the tower dumps span multiple days."

Please see attached opinion and happy Friday!

Jessica

Jessica C. Stone
Vehicular Crimes Training Attorney
Massachusetts District Attorneys Association
One Bulfinch Place, Suite 202
Boston, MA 02114
Office: (617) 305-7032
Mobile: [redacted]
Fax: (617) 367-1228

From: Pack, Noah (POL)
To: Wilcox, Christopher (POL)
Subject: DC Order Draft
Date: Friday, April 29, 2022 11:19:00 AM
Attachments: DC Order Non-Dept ALPR.doc

LTC Wilcox:

Attached is a draft of a Division Commander's Order for your review.

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: Matt O"Brien
To: Bernstein, Eric (POL)
Subject: Dedham Contact for ATS 3
Date: Monday, October 31, 2022 1:40:17 PM
Attachments: ATS 3 & 5 Trailer Brochure.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 Lt. Bernstein,

Town of Dedham Police Department - Michael D'Entremont (Dee-an-tremont) mdentremont@police.dedham-ma.gov, his phone number is 781-603-6159 and he got the Speed Alert 18 ATS 3. The Speed Alert 18 is the one that does the Messaging and Radar (20 inches in height 30 inches wide). If you have any open time slots on November 9th and 10th, I'd be happy to show you the signs we have and answer any and all questions.

Thank you,

Matt

--

Matt O'Brien
Territory Manager CT, MA, ME, NH, RI , VT
Direct: (571) 321-5449, EXT 265
mobrien@alltrafficsolutions.com
All Traffic Solutions
www.AllTrafficSolutions.com

From: Carlo Capano
To: Wilcox, Christopher (POL)
Subject: Digital Brochure
Date: Monday, June 27, 2022 7:36:51 PM
Attachments: Fusus Real-Time Crime Center In The Cloud- 2022 Brochure (1).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.

Sir,

Last is the digital brochure, if you receive this and the price list, that means the PP was the issue. I'll send it in a google drive format.

Carlo

--

Carlo Capano
Director of Sales, Northeast Region
t: +1 844-226-9226 | **m:** +1 (603) [redacted]
w: fusus.com

Fusus Events Calendar: https://www.fusus.com/about-us/fusus-events
Schedule Training: http://fusus.com/training

From:	Warren, Rosemary (POL)
To:	Aumais, Matthew (POL); Bandini, Brian (POL); Boyle, Christopher (DOT); Boyle, Christopher (POL); Brooks, Brian (POL); Bruce, James (POL); Conron, John (POL); Crouse, David (POL); Cunningham, James (POL); Devlin, James (CDA); Dorian, Christine (POL); Driscoll, Francis (POL); Dunn, Scott (POL); Fairchild, Eric (POL); Gavioli, Brian (POL); George, Michael (POL); Goslin, John (POL); Kardoos, Albert (POL); Kaupp, Kevin (POL); LaBarge, Robert (POL); McLaughlin, Kelly (POL); Nason, Nicholas (POL); O"Hara, Edward (POL); OToole, Kevin (POL); Pack, Noah (POL); Popovich, Andrew D (POL); Quigley, Robert (POL); Racki, Steven M (POL); Riley, Patricia (POL); Santos, John (POL); Shink, Norman (POL); Strazzullo, John (POL); Telford, Erik (POL); Thibault, Amy (POL); Twomey, David (POL); Walsh, Mark (POL); Warren, Rosemary (POL)
Cc:	Cyr, Mark (POL); Tucker, Daniel T (POL); Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); McCarthy, Steven (POL)
Subject:	Division Commander"s Orders
Date:	Wednesday, May 18, 2022 3:02:29 PM
Attachments:	DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf DC Order 2022-DHS-003 Unit Commander CCU.pdf

---

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From:	Warren, Rosemary (POL)
To:	Macdonald, Michael (POL); Powers, William (POL); Bresnahan, Geraldine (NWD); Darling, Gary (POL); Richard, Daniel (POL)
Subject:	Draft Documents for Basic Investigator Training
Date:	Tuesday, June 14, 2022 2:47:29 PM
Attachments:	Unattended Death Investigations Updated.pptx Basic Criminal Investigation Class Working Outline.docx Basic Investigator Training AGENDA - Draft.doc

---

Good Afternoon,

Attached are some of the working documents referenced/drafted in the meeting today.

Det. Captain Richard: Please forward to anyone I may have missed that should be included.

Respectfully,

Rose

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

From: Small, Michelle (POL)
To: Sullivan, Margaret (POL)
Subject: DRAFT
Date: Thursday, January 20, 2022 2:51:00 PM
Attachments: MSP IT Project List as Jan 20 22.xlsx

Hi Peg,

I made the updates we discussed. Attached is the updated IT priority list. Please let me know if you would like any additional changes. I would like to send to Maria this evening.

Thank you for your help on this!

-Michelle

Michelle Small
Chief Administrative Officer
Massachusetts State Police
p. 508-820-2366
c. 617-[redacted]

From: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: Draft/Notes for Review
Date: Monday, April 4, 2022 1:29:00 PM
Attachments: SOP DRAFT - Outside LPR.docx
MSP FLOCK MOU.pdf

Sir, please see attached.

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: Pack, Noah (POL)
To: Cyr, Mark (POL)
Subject: DRAFT/NOTES
Date: Tuesday, April 19, 2022 10:02:54 AM
Attachments: TRF-11 Automatic License Plate Recognition DRAFT 13.docx

---

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

To:	ALPR_Support; mroth; Peter Crary; Israel Padilla
Cc:	John Tedona; Egnitz, Brian (POL)
Subject:	Feature Request Update: Historical Search Time Limits and Device Visibility
Date:	Monday, August 8, 2022 8:24:45 PM
Attachments:	group level.PNG

Limit Historical Search Time

We are looking to restrict the amount of historical time that a user can search (ie, the full system retention or a lesser period, say 30 days). This feature request is coming up again because we are preparing to add dispatchers to the system, and we would prefer to restrict their access to a more limited time that is relevant to their duties. I think this makes the most sense to set at the group level (see attached "group level") by selecting to enforce a historical search limit and then entering the allowable days, similar to the hot plate expiration interface. This is a high priority for us.

Set Allowable Devices to See Results

We are still looking to add the ability to set which devices a tenant can see results from. Currently, the searching user in any tenant will see results from every device in the system from all other tenants and can manually see and select from ALL devices from all other tenants. There is no apparent way to restrict this, as we discussed early on during our transition.

Ideally, the system could be set to restrict cross-tenant visibility for devices or sites. This feature request is coming up again due to the addition of more local tenants to the system who we may want to restrict to seeing just their own devices and search results from their own devices as opposed to the entire system. This is probably easiest to set at the tenant level. This is a medium priority for us.

Why is this important?

Building in system level protections to manage user access to the amount and type of data that is relevant to their user group is an important step to protecting the integrity of the system and lowering the potential for accidental misuse.

Thank you. For the agenda to discuss…

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: Pack, Noah (POL)
To: ALPR_Support; mroth; Peter Crary; Israel Padilla
Cc: John Tedona; Egnitz, Brian (POL)
Subject: Feature Request Update: Historical Search Time Limits and Device Visibility
Date: Monday, August 8, 2022 8:29:00 PM
Attachments: group level.PNG

Limit Historical Search Time

We are looking to restrict the amount of historical time that a user can search (ie, the full system retention or a lesser period, say 30 days). This feature request is coming up again because we are preparing to add dispatchers to the system, and we would prefer to restrict their access to a more limited time that is relevant to their duties. I think this makes the most sense to set at the group level (see attached) by selecting to enforce a historical search limit and then entering the allowable days, something similar to the hot plate expiration interface. This is a high priority for us.

Set Allowable Devices to See Results

We are still looking to restrict visibility of devices, including which devices a tenant can see results from. Currently, a searching user in any tenant will by default see results from every device in the system and can manually see and select from ALL devices from all other tenants using the device search filter. There is no apparent way to restrict this, as we discussed in the past during the earlier phase of our boss4 transition.

Ideally, the system should be set to allow administers to restrict cross-tenant visibility for devices or sites. This feature request is coming up again due to the addition of more local tenants to the system who we want to restrict to seeing just their own devices and search results from their own devices as opposed to the entire system. This feature is probably easiest to set at the agency/tenant level. This is a medium priority for us.

Why are these important?

Building in system level protections to manage user access to the amount and type of data that is relevant to their user group is an important step to protecting the integrity of the system and lowering the potential for accidental misuse.

Thank you. Please add to the agenda for our next update meeting.

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:	Jussaume, Carolyn B
To:	Sullivan, Margaret (POL)
Cc:	Michalski, Maria (EPS); Egnitz, Brian (POL); Driscoll, Francis (POL); Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); Paul E Ralston
Subject:	Follow up to discussion on January 13th- Questions related to MDT Image/Security/process/help desk
Date:	Tuesday, January 25, 2022 8:55:28 PM
Attachments:	Verizon Wireless Questions- image provisioning, process, help desk, security.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.

Peg

Thank you for your time on the 13th. Attached is a summary of the questions we discussed. Thank you for your help in clarifying the answers- much appreciated.

Carolyn

--

Carolyn Jussaume

Business Development
Massachusetts Government Team
Verizon Business Group

M 617 [redacted]
100 Causeway Street
Boston, Massachusetts 02114

From:	Carlo Capano
To:	Wilcox, Christopher (POL)
Cc:	Joe Del Duca
Subject:	Following up from request at fusus
Date:	Tuesday, May 31, 2022 3:22:38 PM
Attachments:	Fusus Real-Time Crime Center In The Cloud- 2022 Brochure (1).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 Lt. Colonel Wilcox,

I was just advised that you had called in for a contact over at fusus. First, I want to apologize, I was advised that you had sent in the information online, I'm not sure what happened with that, so my apologies for taking so long to get back to you.

I'm told you were present for my brief overview of fusus at the IACP Tech Conference in Milwaukee, truly appreciate you reaching out. I just wanted to shoot you a quick email, I left you a voice message just a bit ago, please feel free to give me a call or email, whatever is convenient for you. As you know from my introduction in Milwaukee, I'm the retired Chief of Police from Manchester NH and I still live up there, although I grew up in Massachusetts and started my career at West Newbury PD in MA.

As you can see, I have attached Joe Del Duca to this email. Joe is part of the Northeast Team and covers your area. Joe is a retired Deputy Inspector from NYPD, with 28 years experience in Law Enforcement. Both Joe and I are FBINA Grads, I'm from 266 and Joe is from 263, I see you were just before us in 258.

Please feel free to reach out and we will take good care of you!! We would love an opportunity to come down and provide you with a full presentation so you can really see what fusus has to offer and how it can assist your agency. I have attached a digital pamphlet along with this YouTube link:

https://www.youtube.com/watch?v=o9WdtuMVh5E

hopefully it will provide you with some additional information.

Thanks again Lt. Col, We are looking forward to connecting. Appreciate your time and be safe out there,

Carlo

Carlo Capano
Director of Sales, Northeast Region
Chief of Police, Retired, City of Manchester, NH
FBI National Academy, Session 266
FBI LEEDS, 78th Academy
t: +1 844-226-9226 | **m:** +1 (603) [redacted]
w: www.fusus.com

fūsus

To: Mboka-Boyer, Vicky (OGR)
Cc: Rust, Rebecca (POL); Miller, Dianne (POL); Thibault, Amy (POL)
Subject: FSHSP20CFC modification request
Date: Thursday, August 25, 2022 9:21:49 AM
Attachments: QT_MSP081822.1.pdf
Commonwealth_of_Massachusetts_Fusion_Center-Proposal1_copy-i2_-15675-15-Jul-2022-18-14-12.pdf
Est_2524_from_BainCor_Inc._18968.pdf
FSHSP20CFC Modification Request August 2022.docx

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From:	Comeau, Melissa (POL)
To:	Mboka-Boyer, Vicky (OGR)
Cc:	Rust, Rebecca (POL); Miller, Dianne (POL); Thibault, Amy (POL)
Subject:	FSHSP20CFC modification request
Date:	Thursday, August 25, 2022 9:22:13 AM
Attachments:	QT_MSP081822.1.pdf Commonwealth_of_Massachusetts_Fusion_Center-Proposal1_copy-i2_-15675-15-Jul-2022-18-14-12.pdf Est_2524_from_BainCor_Inc._18968.pdf FSHSP20CFC Modification Request August 2022.docx

---

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

To:	Warmington, Scott (POL); Mason, Christopher (POL)
Cc:	Diotte, Jeffrey (POL); Wheeler, Mark (POL)
Subject:	FW:
Date:	Friday, February 11, 2022 1:05:57 PM
Attachments:	draft briefing ULES.zip

Sirs – Just circling back on the proposed LPR meeting. Attached is a draft Power Point that covers our talking points.

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Friday, February 11, 2022 10:07 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject:

Sir, most current draft briefing is attached.

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: Wilcox, Christopher (POL)
To: Warmington, Scott (POL); Mason, Christopher (POL)
Cc: Diotte, Jeffrey (POL); Wheeler, Mark (POL)
Subject: FW:
Date: Friday, February 11, 2022 1:06:25 PM
Attachments: draft briefing ULES.zip

Sirs – Just circling back on the proposed LPR meeting. Attached is a draft Power Point that covers our talking points. We look forward to meeting with you both. CTW

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Friday, February 11, 2022 10:07 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject:

Sir, most current draft briefing is attached.

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: Breck, Kathy
To: Pack, Noah (POL)
Cc: Schwarz, William J; Martucci, J
Subject: FW: [External] RE: [EXTERNAL]ALPR TENANT MOU, with SPD proposed edits, and MSP General Order TRF-11
Date: Friday, June 17, 2022 2:59:51 PM
Attachments: GO 16-03 - ALPR Policy.doc

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.

Dear Sgt. Pack/Noah:

I'm out of the office today, but I spoke with Bill Schwarz earlier and he told me you were at SPD to set up the access to the MSP ALPR.
A few weeks ago SPD Capt. Jeffrey Martucci (copied here) forwarded me the **SPD ALPR Policy** (attached). Is there a way to accommodate both policies in the MOU?
Bill said SPD can wait to start using the MSP system until this is worked out.
Sorry I didn't get back to you sooner- things are crazy busy these days with our fiscal year end. I can pick this back up next Tuesday 6/21 when I'm back in the office.

Best regards,
Kathy Breck 6/17/22

Kathleen T. Breck
Deputy City Solicitor
City of Springfield Law Department
36 Court Street, Room 210
Springfield, MA. 01103
(413)787-6179
kbreck@springfieldcityhall.com

From: Donoghue, William (NOR)
To: Warren, Rosemary (POL)
Cc: Powers, William (POL)
Subject: FW: 2022-2023 Police Training Manual
Date: Monday, November 7, 2022 4:12:27 PM
Attachments: 2022-2023 Police Training Manual.pdf
image001.png

Hi Rose,

Please see attached 2022-2023 Police Training Manual from the Middlesex District Attorney. In speaking with Billy last week thought it would be a good resource for the students in class.

Thanks,

Duke

Detective Lieutenant William J. Donoghue #2341
Massachusetts State Police
Middlesex State Police Detective Unit
15 Commonwealth Avenue
Suite 300
Woburn, MA 01801
781-897-6600

From: Johnsen, Melissa (NOR) <melissa.johnsen@mass.gov>
Sent: Friday, November 04, 2022 2:19 PM
To: Donoghue, William (NOR) <william.j.donoghue@mass.gov>
Subject: 2022-2023 Police Training Manual

Hi Duke,

Here it is – feel free to distribute. We're also ordering hard copies for the office & CPAC, so look for those in the next few weeks. Thanks!

Melissa W. Johnsen, Deputy Chief
Appeals & Training Bureau
Middlesex District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Cell: [redacted]
Desk: 781.897.6838

The preceding email message (including any attachments) contains information that may be confidential, may be protected by they 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 please 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: Donoghue, William (NOR)
To: NOR-DL-ALL CPAC
Subject: FW: 2022-2023 Police Training Manual
Date: Monday, November 7, 2022 4:13:09 PM
Attachments: 2022-2023 Police Training Manual.pdf
image001.png

See attached – great resource!

Detective Lieutenant William J. Donoghue #2341
Massachusetts State Police
Middlesex State Police Detective Unit
15 Commonwealth Avenue
Suite 300
Woburn, MA 01801
781-897-6600

From: Johnsen, Melissa (NOR) <melissa.johnsen@mass.gov>
Sent: Friday, November 04, 2022 2:19 PM
To: Donoghue, William (NOR) <william.j.donoghue@mass.gov>
Subject: 2022-2023 Police Training Manual

Hi Duke,

Here it is – feel free to distribute. We're also ordering hard copies for the office & CPAC, so look for those in the next few weeks. Thanks!

Melissa W. Johnsen, Deputy Chief
Appeals & Training Bureau
Middlesex District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Cell: [redacted]
Desk: 781.897.6838

The preceding email message (including any attachments) contains information that may be confidential, may be protected by they 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 please 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: Rivera Morgan, Awilda (POL)
To: Gabriel, Stephen (POL)
Subject: FW: Admin Rights Requested by Sgt Noah Pack
Date: Thursday, January 20, 2022 1:53:16 PM
Attachments: Exception Request Instructions - Admin Rights.docx
TSS Exception Form - Admin Rights.docx
RE Admin Rights.msg

Here is the information I provided to Major Mill for Admin rights requested by Sgt Pack.

Respectfully,

Awilda Rivera Morgan
Director of Compliance
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508-820-2346 – work direct
M.G.L. c. 4, sec. 7,cl. 26 (c)(privacy) – work cell
awilda riveramorgan@pol.state ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

-----Original Message-----
From: Rivera Morgan, Awilda (POL)
Sent: Monday, November 29, 2021 3:34 PM
To: Mill, John (POL) <john mill@pol.state ma.us>
Cc: Small, Michelle (POL) <Michelle.Small@pol.state.ma.us>
Subject: Admin Rights Requested by Sgt Noah Pack

Major,
We have been informed by EOTSS that Admin Rights need to go through an EOTSS approval process. Attached are the instructions and form that need to be filled out by the user requesting administrator rights. Thank you.

Respectfully,

Awilda Rivera Morgan
Director of Compliance
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508-820-2346 – work direct
M.G.L. c. 4, sec. 7,cl. 26 (c)(privacy) – work cell
awilda riveramorgan@pol.state ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

-----Original Message-----
From: Mill, John (POL) <john mill@pol.state ma.us>
Sent: Monday, November 22, 2021 3:32 PM
To: Rivera Morgan, Awilda (POL) <Awilda.RiveraMorgan@pol.state ma.us>
Subject: FW: Message from "RNP002673B04953"

Good Afternoon Awilda,
Can we please issue Sgt. Noah Pack a cell phone, laptop/docking station/ monitor and keyboard/ VPN and MiFi. Also please have MIS grant him local administrator privileges to allow him to update ALPR software on his laptop.
Thanks,
John

Respectfully Submitted,

Major John A. Mill, Jr. #2550

Major John A. Mill Jr. #2550
Deputy Division Commander
Division of Administrative Services
470 Worcester Road
Framingham, MA 01702
(w) 508-820-2175
(Cell) [redacted]
(Fax) 508-820-2359

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.

-----Original Message-----
From: donotreply@pol.state.ma.us <donotreply@pol.state ma.us>
Sent: Monday, November 22, 2021 3:34 PM
To: Mill, John (POL) <john mill@pol.state ma.us>
Subject: Message from "RNP002673B04953"

This E-mail was sent from "RNP002673B04953" (MP 4054).

Scan Date: 11.22.2021 15:33:39 (-0500)
Queries to: donotreply@pol.state.ma.us

From: Wolanski, Richard Jr. (POL)
To: Cronin, Timothy M. (EOTSS)
Subject: FW: Admin Rights Requested by Sgt Noah Pack
Date: Friday, January 21, 2022 11:10:00 AM
Attachments: Exception Request Instructions - Admin Rights.docx
TSS Exception Form - Admin Rights.docx
RE Admin Rights.msg

Tim,

This is what was sent to me. Any help would be appreciated.

-Rick

Lieutenant Richard D Wolanski, Jr #3203
Section Commander
Collision Analysis & Reconstruction Section
Massachusetts State Police
50 Maple Street
Milford, MA 01757
richard.wolanski@pol.state.ma.us
office: (774) 462-3756

C.A.R.S. Report Requests can be sent to:
cars.reports@state.ma.us

From: Gabriel, Stephen (POL) <stephen.gabriel@pol.state.ma.us>
Sent: Thursday, January 20, 2022 1:57 PM
To: Wolanski, Richard Jr. (POL) <Richard.Wolanski@pol.state.ma.us>
Cc: Monzon, Mario (POL) <mario.monzon@pol.state.ma.us>; Connors, Brian (POL) <Brian.Connors@pol.state.ma.us>
Subject: Fw: Admin Rights Requested by Sgt Noah Pack

Sir,

Please see the attached documents regarding your request for "Admin Rights". Don't hesitate to reach out if you need anything further.

Respectfully,

Major Stephen A. Gabriel, Jr. #2996
Massachusetts State Police
Division of Administrative Services

The Recruitment and Diversity Office

508-820-2175 (office)

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

Essayons

The information transmitted is intended only for the person or entity to which 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: Rivera Morgan, Awilda (POL) <Awilda.RiveraMorgan@pol.state.ma.us>
Sent: Thursday, January 20, 2022 1:53 PM
To: Gabriel, Stephen (POL) <stephen.gabriel@pol.state.ma.us>
Subject: FW: Admin Rights Requested by Sgt Noah Pack

Here is the information I provided to Major Mill for Admin rights requested by Sgt Pack.

Respectfully,

Awilda Rivera Morgan
Director of Compliance
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508-820-2346 – work direct
508-G.L. c. 4, sec. 7,cl. 26 (c) – work cell
awilda.riveramorgan@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

-----Original Message-----

From: Rivera Morgan, Awilda (POL)
Sent: Monday, November 29, 2021 3:34 PM
To: Mill, John (POL) <john.mill@pol.state.ma.us>
Cc: Small, Michelle (POL) <Michelle.Small@pol.state.ma.us>
Subject: Admin Rights Requested by Sgt Noah Pack

Major,
We have been informed by EOTSS that Admin Rights need to go through an EOTSS approval process. Attached are the instructions and form that need to be filled out by the user requesting administrator rights. Thank you.

Respectfully,

Awilda Rivera Morgan
Director of Compliance
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508-820-2346 – work direct
508-[redacted] – work cell
awilda.riveramorgan@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

-----Original Message-----
From: Mill, John (POL) <john.mill@pol.state.ma.us>
Sent: Monday, November 22, 2021 3:32 PM
To: Rivera Morgan, Awilda (POL) <Awilda.RiveraMorgan@pol.state.ma.us>
Subject: FW: Message from "RNP002673B04953"

Good Afternoon Awilda,
Can we please issue Sgt. Noah Pack a cell phone, laptop/docking station/ monitor and keyboard/ VPN and MiFi.
Also please have MIS grant him local administrator privileges to allow him to update ALPR software on his laptop.
Thanks,

John

Respectfully Submitted,

Major John A. Mill, Jr. #2550

Major John A. Mill Jr. #2550
Deputy Division Commander
Division of Administrative Services
470 Worcester Road
Framingham, MA 01702
(w) 508-820-2175
(Cell) 508-[redacted]
(Fax) 508-820-2359

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.

-----Original Message-----
From: donotreply@pol.state.ma.us <donotreply@pol.state.ma.us>
Sent: Monday, November 22, 2021 3:34 PM
To: Mill, John (POL) <john.mill@pol.state.ma.us>
Subject: Message from "RNP002673B04953"

This E-mail was sent from "RNP002673B04953" (MP 4054).

Scan Date: 11.22.2021 15:33:39 (-0500)
Queries to: donotreply@pol.state.ma.us

From: Connor, Debora (POL)
To: McCarthy, Steven (POL); Egnitz, Brian (POL)
Cc: Connor, Debora (POL)
Subject: FW: ALPR & 4RE Decision
Date: Monday, February 28, 2022 11:07:06 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

FYI

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:	Connor, Debora (POL)
To:	Driscoll, Francis (POL)
Cc:	Egnitz, Brian (POL); Connor, Debora (POL)
Subject:	FW: ALPR & 4RE Decision
Date:	Monday, February 28, 2022 11:54:00 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

---

+Lt Driscoll

From: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Sent: Monday, February 28, 2022 11:07 AM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Subject: FW: ALPR & 4RE Decision

FYI

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:	Connor, Debora (POL)
To:	Driscoll, Francis (POL)
Cc:	Egnitz, Brian (POL); Connor, Debora (POL)
Subject:	FW: ALPR and 4RE Email
Date:	Monday, February 28, 2022 11:55:00 AM
Attachments:	APLR and 4RE decision.msg

+Lt Driscoll

From: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Sent: Monday, February 28, 2022 11:11 AM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Subject: ALPR and 4RE Email

FYI

Debora Connor
Special Projects Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-861-6743

The information transmitted is intended only for the person or entity to which 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: Sullivan, Margaret (POL)
To: Sarasin, Ryan (CHS)
Subject: FW: DCJIS Forms
Date: Tuesday, April 26, 2022 12:30:00 PM
Attachments: FW CJIS Agreement.msg

Hi Ryan – Bill Dunn suggested I reach out to you to get a copy of the CJIS Global Sharing Agreement. From reading the attached email thread it appears to be related to an ALPR (license plate reader) vendor. Please let me know if you have questions or need additional information. Thank you for your assistance. -peg

Margaret Sullivan | Executive Office of Public Safety and Security
Director | Application Development and Support Services
Office of Technology and Information Services
470 Worcester Road
Framingham, MA 01702
p. 508-820-2227 | f. 508-820-2359

From: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Sent: Thursday, April 21, 2022 10:52 AM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Subject: RE: DCJIS Forms

I would suggest DCJIS Support (Next week) and ask for Ryan Sarasin
617 660 4710

However, there are a variety of those forms, based on slight differences/requirements

ALPR – License Plate Readers
Sharing RMS Cad
Regional Dispatch Centers
Fire Dept's / Non LE/CJ traversing the routers
Shared (Courtesy Booking) Live Scan

Hope this helps, although likely added more questions to the mix

---

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Thursday, April 21, 2022 10:46 AM
To: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: DCJIS Forms

Hi Bill – I'm hoping you can assist in directing me to the appropriate person at DCJIS who can assist with getting a copy of the most recent version of the attached form. Any assistance you can provide is appreciated. Thanks. -peg

To: Sarasin, Ryan (CHS)
Subject: FW: DCJIS Forms
Date: Tuesday, April 26, 2022 12:15:03 PM
Attachments: FW CJIS Agreement.msg

Hi Ryan – Bill Dunn suggested I reach out to you to get a copy of the

---

From: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Sent: Thursday, April 21, 2022 10:52 AM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Subject: RE: DCJIS Forms

I would suggest DCJIS Support (Next week) and ask for Ryan Sarasin
617 660 4710

However, there are a variety of those forms, based on slight differences/requirements

ALPR – License Plate Readers
Sharing RMS Cad
Regional Dispatch Centers
Fire Dept's / Non LE/CJ traversing the routers
Shared (Courtesy Booking) Live Scan

Hope this helps, although likely added more questions to the mix

---

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Thursday, April 21, 2022 10:46 AM
To: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: DCJIS Forms

Hi Bill – I'm hoping you can assist in directing me to the appropriate person at DCJIS who can assist with getting a copy of the most recent version of the attached form. Any assistance you can provide is appreciated. Thanks. -peg

To: Cormier, Donald (POL)
Subject: FW: DCJIS Forms
Date: Tuesday, June 21, 2022 10:04:51 AM
Attachments: Global Justice Public Safety Agreement FINAL 9-28-2020.docx

---

From: Sarasin, Ryan (CHS) <ryan.sarasin@mass.gov>
Sent: Wednesday, April 27, 2022 12:08 PM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Subject: RE: DCJIS Forms

Good Morning,

Attached is the most recent Global Sharing Agreement. Once the Captain or someone at MSP signs, we can have our DCJIS Commissioner sign off.

-Ryan

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Tuesday, April 26, 2022 12:30 PM
To: Sarasin, Ryan (CHS) <ryan.sarasin@mass.gov>
Subject: FW: DCJIS Forms

Hi Ryan – Bill Dunn suggested I reach out to you to get a copy of the CJIS Global Sharing Agreement. From reading the attached email thread it appears to be related to an ALPR (license plate reader) vendor. Please let me know if you have questions or need additional information. Thank you for your assistance. -peg

Margaret Sullivan | Executive Office of Public Safety and Security
Director | Application Development and Support Services
Office of Technology and Information Services
470 Worcester Road
Framingham, MA 01702
p. 508-820-2227 | f. 508-820-2359

From: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Sent: Thursday, April 21, 2022 10:52 AM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Subject: RE: DCJIS Forms

I would suggest DCJIS Support (Next week) and ask for Ryan Sarasin
617 660 4710

However, there are a variety of those forms, based on slight differences/requirements

ALPR – License Plate Readers
Sharing RMS Cad
Regional Dispatch Centers
Fire Dept's / Non LE/CJ traversing the routers
Shared (Courtesy Booking) Live Scan

Hope this helps, although likely added more questions to the mix

---

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Thursday, April 21, 2022 10:46 AM
To: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: DCJIS Forms

Hi Bill – I'm hoping you can assist in directing me to the appropriate person at DCJIS who can assist with getting a copy of the most recent version of the attached form. Any assistance you can provide is appreciated. Thanks. -peg

From: Commonwealth Fusion Center (POL)
To: Duval, Kaitlyn (POL)
Subject: Fw: Division Commander"s Orders
Date: Monday, October 10, 2022 2:16:14 PM
Attachments: DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf
DC Order 2022-DHS-003 Unit Commander CCU.pdf

Respectfully,

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

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

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:08 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: FW: Division Commander's Orders

From: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:02 PM
To: Aumais, Matthew (POL) <matthew.aumais@pol.state.ma.us>; Bandini, Brian (POL) <brian.bandini@pol.state.ma.us>; Boyle, Christopher (DOT) <Christopher.P.Boyle@dot.state.ma.us>; Boyle, Christopher (POL) <Christopher.Boyle@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Bruce, James (POL) <James.Bruce@pol.state.ma.us>; Conron, John (POL) <john.conron@pol.state.ma.us>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Cunningham, James (POL) <james.cunningham@pol.state.ma.us>; Devlin, James (CDA) <james.devlin@mass.gov>; Dorian, Christine (POL) <Christine.Dorian@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Dunn, Scott (POL) <Scott.Dunn@pol.state.ma.us>; Fairchild, Eric (POL) <eric.fairchild@pol.state.ma.us>; Gavioli, Brian (POL) <brian.gavioli@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Goslin, John (POL) <john.goslin@pol.state.ma.us>; Kardoos, Albert (POL) <albert.kardoos@pol.state.ma.us>; Kaupp, Kevin (POL) <kevin.kaupp@pol.state.ma.us>; LaBarge, Robert (POL) <Robert.LaBarge@pol.state.ma.us>; McLaughlin, Kelly (POL) <kelly.mclaughlin@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; OToole, Kevin (POL) <kevin.otoole@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Popovich, Andrew D (POL) <Andrew.D.Popovich@pol.state.ma.us>; Quigley, Robert (POL) <robert.quigley@pol.state.ma.us>; Racki, Steven M (POL) <Steven.M.Racki@pol.state.ma.us>; Riley, Patricia (POL)

<patricia.riley@pol.state.ma.us>; Santos, John (POL) <john.santos@pol.state.ma.us>; Shink, Norman (POL) <norman.shink@pol.state.ma.us>; Strazzullo, John (POL) <john.strazzullo@pol.state.ma.us>; Telford, Erik (POL) <erik.telford@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Twomey, David (POL) <david.twomey@pol.state.ma.us>; Walsh, Mark (POL) <Mark.Walsh@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Division Commander's Orders

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From: Commonwealth Fusion Center (POL)
To: Salvatore, Justin (POL)
Subject: Fw: Division Commander"s Orders
Date: Monday, May 23, 2022 6:57:02 PM
Attachments: DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf
DC Order 2022-DHS-003 Unit Commander CCU.pdf

Respectfully,

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

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

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:08 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: FW: Division Commander's Orders

From: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:02 PM
To: Aumais, Matthew (POL) <matthew.aumais@pol.state.ma.us>; Bandini, Brian (POL) <brian.bandini@pol.state.ma.us>; Boyle, Christopher (DOT) <Christopher.P.Boyle@dot.state.ma.us>; Boyle, Christopher (POL) <Christopher.Boyle@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Bruce, James (POL) <James.Bruce@pol.state.ma.us>; Conron, John (POL) <john.conron@pol.state.ma.us>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Cunningham, James (POL) <james.cunningham@pol.state.ma.us>; Devlin, James (CDA) <james.devlin@mass.gov>; Dorian, Christine (POL) <Christine.Dorian@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Dunn, Scott (POL) <Scott.Dunn@pol.state.ma.us>; Fairchild, Eric (POL) <eric.fairchild@pol.state.ma.us>; Gavioli, Brian (POL) <brian.gavioli@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Goslin, John (POL) <john.goslin@pol.state.ma.us>; Kardoos, Albert (POL) <albert.kardoos@pol.state.ma.us>; Kaupp, Kevin (POL) <kevin.kaupp@pol.state.ma.us>; LaBarge, Robert (POL) <Robert.LaBarge@pol.state.ma.us>; McLaughlin, Kelly (POL) <kelly.mclaughlin@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; OToole, Kevin (POL) <kevin.otoole@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Popovich, Andrew D (POL) <Andrew.D.Popovich@pol.state.ma.us>; Quigley, Robert (POL) <robert.quigley@pol.state.ma.us>; Racki, Steven M (POL) <Steven.M.Racki@pol.state.ma.us>; Riley, Patricia (POL)

<patricia.riley@pol.state.ma.us>; Santos, John (POL) <john.santos@pol.state.ma.us>; Shink, Norman (POL) <norman.shink@pol.state.ma.us>; Strazzullo, John (POL) <john.strazzullo@pol.state.ma.us>; Telford, Erik (POL) <erik.telford@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Twomey, David (POL) <david.twomey@pol.state.ma.us>; Walsh, Mark (POL) <Mark.Walsh@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Division Commander's Orders

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From: OToole, Kevin (POL)
To: Shink, Norman (POL)
Cc: Plante, Michelle (POL)
Subject: Fw: Division Commander"s Orders
Date: Wednesday, May 18, 2022 3:11:16 PM
Attachments: DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf
Outlook-r2bp33jo.png

---

see attached

Respectfully Submitted,
Detective Lieutenant Kevin A. O'Toole #2768
Massachusetts State Police
Commonwealth Interstate Narcotics Reduction Enforcement Team (C.I.N.R.E.T) WEST Unit Commander
53 Elliot Street
Springfield, MA 01105
Mobile: ([redacted]

From: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:02 PM
To: Aumais, Matthew (POL) <matthew.aumais@pol.state.ma.us>; Bandini, Brian (POL) <brian.bandini@pol.state.ma.us>; Boyle, Christopher (DOT) <Christopher.P.Boyle@dot.state.ma.us>; Boyle, Christopher (POL) <Christopher.Boyle@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Bruce, James (POL) <James.Bruce@pol.state.ma.us>; Conron, John (POL) <john.conron@pol.state.ma.us>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Cunningham, James (POL) <james.cunningham@pol.state.ma.us>; Devlin, James (CDA) <james.devlin@mass.gov>; Dorian, Christine (POL) <Christine.Dorian@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Dunn, Scott (POL) <Scott.Dunn@pol.state.ma.us>; Fairchild, Eric (POL) <eric.fairchild@pol.state.ma.us>; Gavioli, Brian (POL) <brian.gavioli@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Goslin, John (POL) <john.goslin@pol.state.ma.us>; Kardoos, Albert (POL) <albert.kardoos@pol.state.ma.us>; Kaupp, Kevin (POL) <kevin.kaupp@pol.state.ma.us>; LaBarge, Robert (POL) <Robert.LaBarge@pol.state.ma.us>; McLaughlin, Kelly (POL) <kelly.mclaughlin@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; OToole, Kevin (POL) <kevin.otoole@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Popovich, Andrew D (POL) <Andrew.D.Popovich@pol.state.ma.us>; Quigley, Robert (POL) <robert.quigley@pol.state.ma.us>; Racki, Steven M (POL) <Steven.M.Racki@pol.state.ma.us>; Riley, Patricia (POL) <patricia.riley@pol.state.ma.us>; Santos, John (POL) <john.santos@pol.state.ma.us>; Shink, Norman (POL) <norman.shink@pol.state.ma.us>; Strazzullo, John (POL) <john.strazzullo@pol.state.ma.us>;

Telford, Erik (POL) <erik.telford@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Twomey, David (POL) <david.twomey@pol.state.ma.us>; Walsh, Mark (POL) <Mark.Walsh@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Division Commander's Orders

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From: Commonwealth Fusion Center (POL)
To: O"Hara, Edward (POL)
Subject: Fw: Division Commander"s Orders
Date: Monday, October 10, 2022 2:16:31 PM
Attachments: DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf
DC Order 2022-DHS-003 Unit Commander CCU.pdf

Respectfully,

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

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

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:08 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: FW: Division Commander's Orders

From: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Sent: Wednesday, May 18, 2022 3:02 PM
To: Aumais, Matthew (POL) <matthew.aumais@pol.state.ma.us>; Bandini, Brian (POL) <brian.bandini@pol.state.ma.us>; Boyle, Christopher (DOT) <Christopher.P.Boyle@dot.state.ma.us>; Boyle, Christopher (POL) <Christopher.Boyle@pol.state.ma.us>; Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Bruce, James (POL) <James.Bruce@pol.state.ma.us>; Conron, John (POL) <john.conron@pol.state.ma.us>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Cunningham, James (POL) <james.cunningham@pol.state.ma.us>; Devlin, James (CDA) <james.devlin@mass.gov>; Dorian, Christine (POL) <Christine.Dorian@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Dunn, Scott (POL) <Scott.Dunn@pol.state.ma.us>; Fairchild, Eric (POL) <eric.fairchild@pol.state.ma.us>; Gavioli, Brian (POL) <brian.gavioli@pol.state.ma.us>; George, Michael (POL) <Michael.George@pol.state.ma.us>; Goslin, John (POL) <john.goslin@pol.state.ma.us>; Kardoos, Albert (POL) <albert.kardoos@pol.state.ma.us>; Kaupp, Kevin (POL) <kevin.kaupp@pol.state.ma.us>; LaBarge, Robert (POL) <Robert.LaBarge@pol.state.ma.us>; McLaughlin, Kelly (POL) <kelly.mclaughlin@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; O'Hara, Edward (POL) <Edward.OHara@pol.state.ma.us>; OToole, Kevin (POL) <kevin.otoole@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Popovich, Andrew D (POL) <Andrew.D.Popovich@pol.state.ma.us>; Quigley, Robert (POL) <robert.quigley@pol.state.ma.us>; Racki, Steven M (POL) <Steven.M.Racki@pol.state.ma.us>; Riley, Patricia (POL)

<patricia.riley@pol.state.ma.us>; Santos, John (POL) <john.santos@pol.state.ma.us>; Shink, Norman (POL) <norman.shink@pol.state.ma.us>; Strazzullo, John (POL) <john.strazzullo@pol.state.ma.us>; Telford, Erik (POL) <erik.telford@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Twomey, David (POL) <david.twomey@pol.state.ma.us>; Walsh, Mark (POL) <Mark.Walsh@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>; Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>; Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Division Commander's Orders

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From:	kblackwell@attleboropolice.org
To:	Pack, Noah (POL)
Subject:	FW: Emailing: 2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement
Date:	Thursday, July 28, 2022 1:57:53 PM
Attachments:	2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement.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,

Please see our signed copy of the MOU for the LPR's. Is there anything else that will be required of our agency to have access the hot list and other functions needed to get us back up and running?

Thanks,
Sgt. K. Blackwell

-----Original Message-----
From: kheagney@attleboropolice.org <kheagney@attleboropolice.org>
Sent: Thursday, July 28, 2022 1:54 PM
To: kblackwell@attleboropolice.org
Subject: Emailing: 2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement

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

2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement

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.

Sergeant Kevin S. Blackwell

"There is always a better way."
Thomas Edison

KBlackwell@attleboropolice.org
(508)942-6616

From:	kblackwell@attleboropolice.org
To:	Pack, Noah (POL)
Subject:	FW: Emailing: 2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement
Date:	Thursday, August 18, 2022 10:55:19 AM
Attachments:	2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement.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,

Just following up on the last email. Is there anything else we need to be fully back up with our LPR's? Also looking for access to manage our users accounts. We have several new Officers that need to be able to use them, as well I would like to remove any that are no longer with our agency.

Thanks,
Sgt. K. Blackwell

-----Original Message-----
From: kblackwell@attleboropolice.org <kblackwell@attleboropolice.org>
Sent: Thursday, July 28, 2022 1:57 PM
To: 'Pack, Noah (POL)' <noah.pack@state.ma.us>
Subject: FW: Emailing: 2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement

Sgt. Pack,

Please see our signed copy of the MOU for the LPR's. Is there anything else that will be required of our agency to have access the hot list and other functions needed to get us back up and running?

Thanks,
Sgt. K. Blackwell

-----Original Message-----
From: kheagney@attleboropolice.org <kheagney@attleboropolice.org>
Sent: Thursday, July 28, 2022 1:54 PM
To: kblackwell@attleboropolice.org
Subject: Emailing: 2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement

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

2022 Automated License Plate Recognition (ALPR) System SP and PD Memorandum of Understanding and Agreement

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.

Sergeant Kevin S. Blackwell

"There is always a better way."
Thomas Edison

KBlackwell@attleboropolice.org
(508)942-6616

From:	Wilcox, Christopher (POL)
To:	Crouse, David (POL)
Subject:	Fw: Following up from request at fusus
Date:	Wednesday, June 1, 2022 10:44:46 AM
Attachments:	Fusus Real-Time Crime Center In The Cloud- 2022 Brochure (1).pdf

---

From: Carlo Capano <ctc@fusus.com>
Sent: Tuesday, May 31, 2022 3:20 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Cc: Joe Del Duca <jld@fusus.com>
Subject: Following up from request at fusus

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 Lt. Colonel Wilcox,

I was just advised that you had called in for a contact over at fusus. First, I want to apologize, I was advised that you had sent in the information online, I'm not sure what happened with that, so my apologies for taking so long to get back to you.

I'm told you were present for my brief overview of fusus at the IACP Tech Conference in Milwaukee, truly appreciate you reaching out. I just wanted to shoot you a quick email, I left you a voice message just a bit ago, please feel free to give me a call or email, whatever is convenient for you. As you know from my introduction in Milwaukee, I'm the retired Chief of Police from Manchester NH and I still live up there, although I grew up in Massachusetts and started my career at West Newbury PD in MA.

As you can see, I have attached Joe Del Duca to this email. Joe is part of the Northeast Team and covers your area. Joe is a retired Deputy Inspector from NYPD, with 28 years experience in Law Enforcement. Both Joe and I are FBINA Grads, I'm from 266 and Joe is from 263, I see you were just before us in 258.

Please feel free to reach out and we will take good care of you!! We would love an opportunity to come down and provide you with a full presentation so you can really see what fusus has to offer and how it can assist your agency. I have attached a digital pamphlet along with this YouTube link:

https://www.youtube.com/watch?v=o9WdtuMVh5E

hopefully it will provide you with some additional information.

Thanks again Lt. Col, We are looking forward to connecting. Appreciate your time and be safe out there,

Carlo

Carlo Capano
Director of Sales, Northeast Region

Chief of Police, Retired, City of Manchester, NH
FBI National Academy, Session 266
FBI LEEDS, 78th Academy
t: +1 844-226-9226 | **m:** +1 (603) [redacted]
w: www.fusus.com

fūsus

From: Wilcox, Christopher (POL)
To: Green, Brian (POL)
Subject: Fw: Following up from request at fusus
Date: Monday, June 6, 2022 3:18:37 PM
Attachments: Fusus Real-Time Crime Center In The Cloud- 2022 Brochure (1).pdf

---

Here is the information on FUSUS

From: Carlo Capano <ctc@fusus.com>
Sent: Tuesday, May 31, 2022 3:20 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Cc: Joe Del Duca <jld@fusus.com>
Subject: Following up from request at fusus

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 Lt. Colonel Wilcox,

I was just advised that you had called in for a contact over at fusus. First, I want to apologize, I was advised that you had sent in the information online, I'm not sure what happened with that, so my apologies for taking so long to get back to you.

I'm told you were present for my brief overview of fusus at the IACP Tech Conference in Milwaukee, truly appreciate you reaching out. I just wanted to shoot you a quick email, I left you a voice message just a bit ago, please feel free to give me a call or email, whatever is convenient for you. As you know from my introduction in Milwaukee, I'm the retired Chief of Police from Manchester NH and I still live up there, although I grew up in Massachusetts and started my career at West Newbury PD in MA.

As you can see, I have attached Joe Del Duca to this email. Joe is part of the Northeast Team and covers your area. Joe is a retired Deputy Inspector from NYPD, with 28 years experience in Law Enforcement. Both Joe and I are FBINA Grads, I'm from 266 and Joe is from 263, I see you were just before us in 258.

Please feel free to reach out and we will take good care of you!! We would love an opportunity to come down and provide you with a full presentation so you can really see what fusus has to offer and how it can assist your agency. I have attached a digital pamphlet along with this YouTube link:

https://www.youtube.com/watch?v=o9WdtuMVh5E

hopefully it will provide you with some additional information.

Thanks again Lt. Col, We are looking forward to connecting. Appreciate your time and be safe out there,

Carlo

Carlo Capano
Director of Sales, Northeast Region

Chief of Police, Retired, City of Manchester, NH
FBI National Academy, Session 266
FBI LEEDS, 78th Academy
t: +1 844-226-9226 | **m:** +1 (603) [redacted]
w: www.fusus.com

fūsus

From: Miller, Dianne (POL)
To: Comeau, Melissa (POL)
Subject: FW: FSHSP20CFC modification request
Date: Wednesday, September 28, 2022 2:44:00 PM
Attachments: image001.png
FSHSP20CFC FFY20 ISA POL CFC - ISA.doc

FYI
I'll review this on Friday and check equipment vs. the initial ISA.
I'll check MMARS BQ89 to see if there's a carryforward, maybe you can check too?
Thx

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 12:29 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
Thanks – attached is the ISA moving items into equipment and UU.

The Bain quote looks like KK and the software and ALPR's, UU – do you agree?

If so, can you double check the attached?

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:53 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

I think she's decreasing AA and increasing UU.
So we need to make sure the UU total in column I adds up to what her quotes were for, and match her modification request letter.
Sorry, I didn't realize no carryforward was done. There's a spreadsheet in the V drive for carryforward so I assumed it was done.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:47 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
The carryforward has not been processed yet. They only did a blanket 90,000 back in June.

If we are carrying forward what was budgeted, I will re-work attachment B to adjust for the change in payroll tax, indirect, and fringe. Do you know if Amy wants to change any of the budgeted amounts in each category? I initially kept it blank as I didn't know if Amy wanted to adjust the categories.

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 10:45 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi again,
If a carryforward was already processed by EOPSS, then column E for FY22 would have the actual amounts you have in Column I.
And the amounts in column G are the starting point for FY23 in column E (for example, AA should have 10563.39, EE conference space should start with $5K in column E ….etc)
Unless I'm mistaken….I think that's how we would do it. Then add & subtract FY23 lines as needed to get to Amy's modified budget in column I.
Di

From: Miller, Dianne (POL)
Sent: Tuesday, September 27, 2022 4:31 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Questions…
Becky, attached is a carryforward that was already processed?
If yes, I think the carryforward amounts from column G are the starting point in column E for FY23….then show the increases and decreases that result in Column I amounts for Amy to spend down.

Amy…is this a good time to attach a food quote for the faith-based seminar and make sure it's approved? There's $5K for conference space, so maybe we can incorporate it all and make sure it's covered?
Vicky already has your equipment quotes so maybe it's not a good idea to attach another one. Just a thought.

[See instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Am Afte Amendn
2022	8000-4692	AA	Salary	$59,133.39	-	$10563.39		$48570.00
2022	8000-4692	BB	Travel	$100,000	-	$94103.28		$5896.72
2022	8000-4692	CC	Contractor Services	$149,000	-	$73351.25		$75648.75
2022	8000-4692	DD	Payroll Tax @ $1.97%	$6198.31	-	$3572.04		$2626.27
2022	8000-4692	DD	Fringe @ 37.46%	$22151.37	-	$413.85		$18014.52
2022	8000-4692	EE	Indirect Cost @ 17.55%	$10377.91	-	$1853.86		$8524.05
2022	8000-4692	EE	Conference Space	$5000	-	$5000		$0
2022	8000-4692	EE	Supplies	$21467.5	-	$1548.50		$23016
2022	8000-4692	UU	IT Software	$120245.50	-	$120245.50		$0
2023	8000-4692	AA	Salary					
2023	8000-4692	BB	Travel					
2023	8000-4692	CC	Contractor Services	$106,426.02				
2023	8000-4692	DD	Payroll Tax @ $1.97%					
2023	8000-4692	DD	Fringe @ 37.46%					
2023	8000-4692	EE	Indirect Cost @ 17.55%					
2023	8000-4692	EE	Conference Space			$		$
2023	8000-4692	EE	Supplies			$		$
2023	8000-4692	UU	IT Software	$150,000.00				

Di

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 22, 2022 1:08 PM

To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Please see the completed Attachment A. Thank you both.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 2:00 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

The attachment B has been populated. I updated the FY22 numbers to match what is in MMARS. The total for FY22 is $186,296.31.

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?
Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research

Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM

To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

Subject: FW: FSHSP20CFC modification request
Date: Wednesday, September 28, 2022 1:41:11 PM
Attachments: image001.png
FSHSP20CFC FFY20 ISA POL CFC - ISA.doc

From: Rust, Rebecca (POL)
Sent: Wednesday, September 28, 2022 12:29 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
Thanks – attached is the ISA moving items into equipment and UU.

The Bain quote looks like KK and the software and ALPR's, UU – do you agree?

If so, can you double check the attached?

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:53 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

I think she's decreasing AA and increasing UU.
So we need to make sure the UU total in column I adds up to what her quotes were for, and match her modification request letter.
Sorry, I didn't realize no carryforward was done. There's a spreadsheet in the V drive for carryforward so I assumed it was done.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:47 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
The carryforward has not been processed yet. They only did a blanket 90,000 back in June.

If we are carrying forward what was budgeted, I will re-work attachment B to adjust for the change in payroll tax, indirect, and fringe. Do you know if Amy wants to change any of the budgeted amounts in each category? I initially kept it blank as I didn't know if Amy wanted to adjust the categories.

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 10:45 AM

To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi again,
If a carryforward was already processed by EOPSS, then column E for FY22 would have the actual amounts you have in Column I.
And the amounts in column G are the starting point for FY23 in column E (for example, AA should have 10563.39, EE conference space should start with $5K in column E ….etc)
Unless I'm mistaken….I think that's how we would do it. Then add & subtract FY23 lines as needed to get to Amy's modified budget in column I.
Di

From: Miller, Dianne (POL)
Sent: Tuesday, September 27, 2022 4:31 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Questions…
Becky, attached is a carryforward that was already processed?
If yes, I think the carryforward amounts from column G are the starting point in column E for FY23….then show the increases and decreases that result in Column I amounts for Amy to spend down.

Amy…is this a good time to attach a food quote for the faith-based seminar and make sure it's approved? There's $5K for conference space, so maybe we can incorporate it all and make sure it's covered?
Vicky already has your equipment quotes so maybe it's not a good idea to attach another one. Just a thought.

[See instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A	B	C	D	E	F	G	H	I
Budget Fiscal Year	**Seller/Child Account**	**Object Class**	**Description**	**Initial ISA Amount / or Amount Prior to Amendment**	**Indicate Add or Reduce +/-**	**Amendment Amount**	**Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds**	**New Am After Amendn**
2022	8000-4692	AA	Salary	$59,133.39	-	$10563.39		$48570.00
2022	8000-4692	BB	Travel	$100,000	-	$94103.28		$5896.72
2022	8000-4692	CC	Contractor Services	$149,000	-	$73351.25		$75648.75
2022	8000-4692	DD	Payroll Tax @ $1.97%	$6198.31	-	$3572.04		$2626.27
2022	8000-4692	DD	Fringe @ 37.46%	$22151.37	-	$413.85		$18014.52
2022	8000-4692	EE	Indirect Cost @ 17.55%	$10377.91	-	$1853.86		$8524.05
2022	8000-4692	EE	Conference Space	$5000	-	$5000		$0
2022	8000-4692	EE	Supplies	$21467.5	-	$1548.50		$23016
2022	8000-4692	UU	IT Software	$120245.50	-	$120245.50		$0
2023	8000-4692	AA	Salary					
2023	8000-4692	BB	Travel					
2023	8000-4692	CC	Contractor Services	$106,426.02				
2023	8000-4692	DD	Payroll Tax @ $1.97%					
2023	8000-4692	DD	Fringe @ 37.46%					
2023	8000-4692	EE	Indirect Cost @ 17.55%					
2023	8000-4692	EE	Conference Space			$		$
2023	8000-4692	EE	Supplies			$		$
2023	8000-4692	UU	IT Software	$150,000.00				

Di

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 22, 2022 1:08 PM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Please see the completed Attachment A. Thank you both.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 2:00 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

The attachment B has been populated. I updated the FY22 numbers to match what is in MMARS. The total for FY22 is $186,296.31.

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?
Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>

Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Rust, Rebecca (POL)
To: Comeau, Melissa (POL)
Subject: FW: FSHSP20CFC modification request
Date: Wednesday, September 28, 2022 1:41:00 PM
Attachments: FSHSP20CFC FFY20 ISA POL CFC - ISA.doc

Attached

From: Rust, Rebecca (POL)
Sent: Wednesday, September 28, 2022 12:29 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
Thanks – attached is the ISA moving items into equipment and UU.

The Bain quote looks like KK and the software and ALPR's, UU – do you agree?

If so, can you double check the attached?

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?

Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road

Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Miller, Dianne (POL)
To: Comeau, Melissa (POL); Rust, Rebecca (POL)
Subject: FW: FSHSP20CFC modification request
Date: Monday, October 3, 2022 7:45:00 PM
Attachments: image001.png
FSHSP20CFC FFY20 ISA POL CFC - ISA.doc

Hi Melissa,
Becky did the carryforward correctly last week…sorry Becky. I was thinking we needed to carry all the amounts forward to the same category first, and then modify.
In the past we used UU for solar trailers but KK makes sense too.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 12:29 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
Thanks – attached is the ISA moving items into equipment and UU.

The Bain quote looks like KK and the software and ALPR's, UU – do you agree?

If so, can you double check the attached?

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:53 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

I think she's decreasing AA and increasing UU.
So we need to make sure the UU total in column I adds up to what her quotes were for, and match her modification request letter.
Sorry, I didn't realize no carryforward was done. There's a spreadsheet in the V drive for carryforward so I assumed it was done.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:47 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
The carryforward has not been processed yet. They only did a blanket 90,000 back in June.

If we are carrying forward what was budgeted, I will re-work attachment B to adjust for the change in payroll tax, indirect, and fringe. Do you know if Amy wants to change any of the budgeted amounts in each category? I initially kept it blank as I didn't know if Amy wanted to adjust the categories.

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 10:45 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi again,
If a carryforward was already processed by EOPSS, then column E for FY22 would have the actual amounts you have in Column I.
And the amounts in column G are the starting point for FY23 in column E (for example, AA should have 10563.39, EE conference space should start with $5K in column E ….etc)
Unless I'm mistaken….I think that's how we would do it. Then add & subtract FY23 lines as needed to get to Amy's modified budget in column I.
Di

From: Miller, Dianne (POL)
Sent: Tuesday, September 27, 2022 4:31 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Questions…
Becky, attached is a carryforward that was already processed?
If yes, I think the carryforward amounts from column G are the starting point in column E for FY23….then show the increases and decreases that result in Column I amounts for Amy to spend down.

Amy…is this a good time to attach a food quote for the faith-based seminar and make sure it's approved? There's $5K for conference space, so maybe we can incorporate it all and make sure it's covered?
Vicky already has your equipment quotes so maybe it's not a good idea to attach another one. Just a thought.

[See instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Am After Amendn
2022	8000-4692	AA	Salary	$59,133.39	-	$10563.39		$48570.00
2022	8000-4692	BB	Travel	$100,000	-	$94103.28		$5896.72
2022	8000-4692	CC	Contractor Services	$149,000	-	$73351.25		$75648.75
2022	8000-4692	DD	Payroll Tax @ $1.97%	$6198.31	-	$3572.04		$2626.27
2022	8000-4692	DD	Fringe @ 37.46%	$22151.37	-	$413.85		$18014.52
2022	8000-4692	EE	Indirect Cost @ 17.55%	$10377.91	-	$1853.86		$8524.05
2022	8000-4692	EE	Conference Space	$5000	-	$5000		$0
2022	8000-4692	EE	Supplies	$21467.5	+	$1548.50		$23016
2022	8000-4692	UU	IT Software	$120245.50	-	$120245.50		$0
2023	8000-4692	AA	Salary					
2023	8000-4692	BB	Travel					
2023	8000-4692	CC	Contractor Services	$106,426.02				
2023	8000-4692	DD	Payroll Tax @ $1.97%					
2023	8000-4692	DD	Fringe @ 37.46%					
2023	8000-4692	EE	Indirect Cost @ 17.55%					
2023	8000-4692	EE	Conference Space			$		$
2023	8000-4692	EE	Supplies			$		$
2023	8000-4692	UU	IT Software	$150,000.00				

Di

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 22, 2022 1:08 PM

To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Please see the completed Attachment A. Thank you both.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 2:00 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

The attachment B has been populated. I updated the FY22 numbers to match what is in MMARS. The total for FY22 is $186,296.31.

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?
Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research

Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM

To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Cormier, Donald (POL)
To: Pack, Noah (POL)
Subject: FW: Global Justice Public Safety Agreement
Date: Thursday, May 5, 2022 12:21:52 PM
Attachments: Global Justice Public Safety Agreement FINAL 9-28-2020.docx

---

Noah,

Is this what you are looking for regarding MOU for the contractor? Capt. Cormier

---

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Thursday, May 05, 2022 12:19 PM
To: Cormier, Donald (POL) <donald.cormier@pol.state.ma.us>
Subject: Global Justice Public Safety Agreement

Hello Capt. Cormier – Attached is the most recent Global Sharing Agreement. Once it is signed by MSP, it needs to be returned to DCJIS for the Commissioner's signature. Let me know if you have questions. -peg

Margaret Sullivan | Executive Office of Public Safety and Security
Director | Application Development and Support Services
Office of Technology and Information Services
470 Worcester Road
Framingham, MA 01702
p. 508-820-2227 | f. 508-820-2359

To: Tucker, Daniel T (POL)
Cc: Anderson, Brian (POL)
Bcc: Bender, Sean (POL)
Subject: FW: Hotlists for Troop Dispatch
Date: Tuesday, August 30, 2022 1:53:42 PM
Attachments: image.png
image001.png

Major, please see IA Bender's response below in which I think he makes excellent points. Before I respond to Sgt. Pack, I'd like to discuss with you Sgt. Packs suggestions. Respectfully, Brian

Lieutenant Brian Brooks
Commonwealth Fusion Center – Watch Center
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2233

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, August 30, 2022 7:58 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Subject: Re: Hotlists for Troop Dispatch

Good Morning, Sir -

*Weighing in because Justin is off for a couple of days and Lt. Brooks is not in yet. I don't want you to think we're all ignoring your email!

In looking through the plates currently in the various Troop Dispatch hotlists, it looks like most folks are generally utilizing the default expiration date when entering a plate. I will send out a reminder to our Analytical Staff to exercise some discretion/common sense when entering hotlists for Dispatch BOLOs.

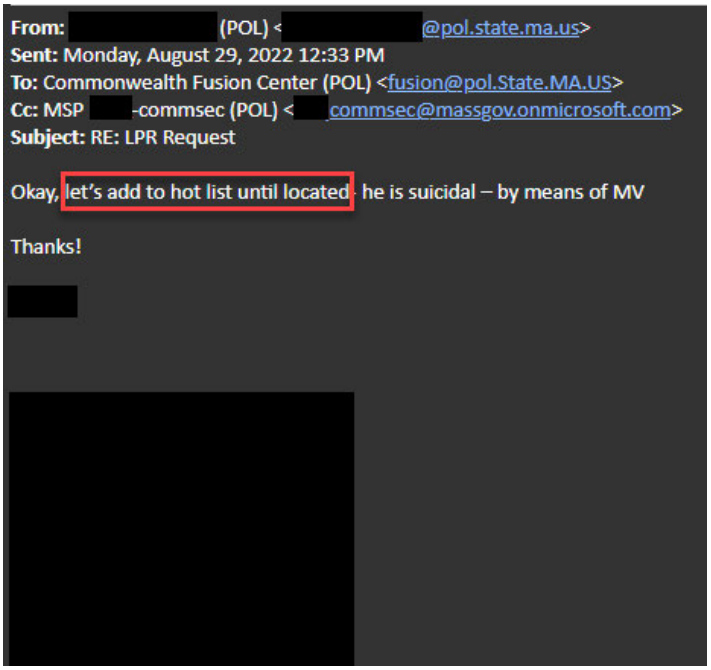
As you are aware, some of the Troop Dispatch centers have developed strong opinions about the appropriate usage of the ALPR system. I certainly agree that in a perfect world, our Analytical Staff would be able to exercise 'best judgement' in setting hotlist expiration dates,

and a written policy would go a long way towards giving us some leverage to push back on requests that don't meet whatever threshold is decided on.

An example we received yesterday:

Missing / Potentially Q5 Party

- 12:29 - Request from Troop Dispatch for historical data
- 12:31 - CFC Response: No hits within past 24 hours
- 12:33 - Request from Troop Dispatch for hotlist (see below):



- 12:37 - After discussion between myself and the Analyst handling the request, we settled on a hotlist for 24 hours with the justification that if 24 hours pass, the party will likely either be located, or the Q5 risk will have been mitigated/unsubstantiated.
- 13:15 - Subject located.

In this case, the requestor asked for a hotlist 'until the subject is located'. TTL in this case ended up being less than an hour, so there was absolutely no need for a 30 day hotlist and 24 hours ended up being *more* than sufficient, possibly even still excessive.

My issue with a request like this is that we are trying to balance accommodating the requestor while also exercising an appropriate level of discretion. Without a written policy to cite, we don't have a lot of protection with which to push back, as evidenced by some of our recent issues and complaints we have received with the level of assistance rendered. We put that Q5 plate on a 24 hour hotlist. If that hotlist expires and the party hits on the LPR at hour 25 and kills themselves or somebody else at hour 26, we're in the glue because the requestor asked for a longer date and we exercised discretion to overrule them.

In absence of an updated written policy a la TRF-11, I think it would be very beneficial to have some of the Dispatch Centers who want to utilize the LPR system either directly or through the CFC, receive some training on authorized/appropriate usage and/or guidelines for submitting LPR requests.

Respectfully,

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, August 27, 2022 7:48 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>; Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: Hotlists for Troop Dispatch

Sirs:

We are working on training and guidelines for dispatchers regarding LPR, and I'm looking for your feedback. At present, when a troop dispatch asks to put a license plate on a hotlist, please vet the reason for the entry and select the expiration date accordingly. (Do you do this now, or do you generally just enter it for the default period?) In many cases, such as when entering BOLOs or info for agencies reporting a real time event, **hotlist entry expiration of 24 hours or less is likely appropriate.** Recall that the default expiration date is 30 days unless adjusted when entering the plate. Leaving a stale BOLO in a dispatch hotlist, which could result in a broadcast to Troopers when the vehicle is no longer wanted or sought, is a situation we seek to avoid.

Example 1: a BOLO is put out for a vehicle involved in a shooting in Springfield. This matter will be investigated by Springfield PD, and they have access to the LPR system or can contact CFC/CWC directly to use it in their investigation. The active life of this BOLO is probably not more than a few hours or end of the working crew's shift, unless circumstances dictate otherwise.

Information changes quickly, and it is the responsibility (by policy) of the members entering or requesting the entries to remove them when no longer needed. It is not the duty of our dispatchers to stay abreast of ongoing investigations. Since they may be unaware if a plate needs to stay on the hotlist, it follows that they generally should not be requesting hotlist entries for an extended period of time.

Example 2: Brockton PD broadcasts info on a recently stolen vehicle. This vehicle hasn't yet been entered into NCIC. The active life of this BOLO is also probably not more than a few hours or end of

the working crew's shift. The vehicle will be entered into NCIC (and removed by the ORI when no longer stolen). Manual hotlist entries are not intended to serve as a long term means to identify and broadcast motor vehicle offenses over troop radios.

Please let know your thoughts on this, including any other common scenarios you find when field inquiries from dispatch. Once we get the appropriate guidelines here, we can push it out to your team and to the dispatchers in their training.

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: Brooks, Brian (POL)
To: Tucker, Daniel T (POL)
Subject: FW: Hotlists for Troop Dispatch
Date: Tuesday, August 30, 2022 2:06:00 PM
Attachments: image.png
image001.png

Major, please see IA Bender's response below in which I think he makes excellent points. Before I respond to Sgt. Pack, I'd like to discuss with you Sgt. Packs suggestions. Respectfully, Brian

Lieutenant Brian Brooks
Commonwealth Fusion Center – Watch Center
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2233

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, August 30, 2022 7:58 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Subject: Re: Hotlists for Troop Dispatch

Good Morning, Sir -

*Weighing in because Justin is off for a couple of days and Lt. Brooks is not in yet. I don't want you to think we're all ignoring your email!

In looking through the plates currently in the various Troop Dispatch hotlists, it looks like most folks are generally utilizing the default expiration date when entering a plate. I will send out a reminder to our Analytical Staff to exercise some discretion/common sense when entering hotlists for Dispatch BOLOs.

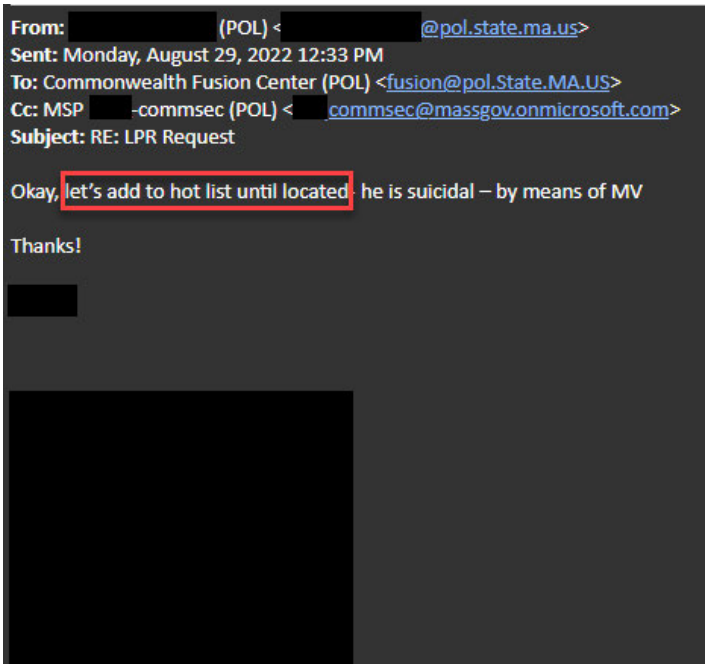
As you are aware, some of the Troop Dispatch centers have developed strong opinions about the appropriate usage of the ALPR system. I certainly agree that in a perfect world, our Analytical Staff would be able to exercise 'best judgement' in setting hotlist expiration dates, and a written policy would go a long way towards giving us some leverage to push back on

requests that don't meet whatever threshold is decided on.

An example we received yesterday:

Missing / Potentially Q5 Party

- 12:29 - Request from Troop Dispatch for historical data
- 12:31 - CFC Response: No hits within past 24 hours
- 12:33 - Request from Troop Dispatch for hotlist (see below):


From: [redacted] (POL) <[redacted]@pol.state.ma.us>
Sent: Monday, August 29, 2022 12:33 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: MSP [redacted]-commsec (POL) <[redacted]commsec@massgov.onmicrosoft.com>
Subject: RE: LPR Request

Okay, let's add to hot list until located - he is suicidal – by means of MV

Thanks!

[redacted]

[redacted]

- 12:37 - After discussion between myself and the Analyst handling the request, we settled on a hotlist for 24 hours with the justification that if 24 hours pass, the party will likely either be located, or the Q5 risk will have been mitigated/unsubstantiated.
- 13:15 - Subject located.

In this case, the requestor asked for a hotlist 'until the subject is located'. TTL in this case ended up being less than an hour, so there was absolutely no need for a 30 day hotlist and 24 hours ended up being *more* than sufficient, possibly even still excessive.

My issue with a request like this is that we are trying to balance accommodating the requestor while also exercising an appropriate level of discretion. Without a written policy to cite, we don't have a lot of protection with which to push back, as evidenced by some of our recent issues and complaints we have received with the level of assistance rendered. We put that Q5 plate on a 24 hour hotlist. If that hotlist expires and the party hits on the LPR at hour 25 and kills themselves or somebody else at hour 26, we're in the glue because the requestor asked for a longer date and we exercised discretion to overrule them.

In absence of an updated written policy a la TRF-11, I think it would be very beneficial to have

some of the Dispatch Centers who want to utilize the LPR system either directly or through the CFC, receive some training on authorized/appropriate usage and/or guidelines for submitting LPR requests.

Respectfully,

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, August 27, 2022 7:48 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>; Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: Hotlists for Troop Dispatch

Sirs:

We are working on training and guidelines for dispatchers regarding LPR, and I'm looking for your feedback. At present, when a troop dispatch asks to put a license plate on a hotlist, please vet the reason for the entry and select the expiration date accordingly. (Do you do this now, or do you generally just enter it for the default period?) In many cases, such as when entering BOLOs or info for agencies reporting a real time event, **hotlist entry expiration of 24 hours or less is likely appropriate.** Recall that the default expiration date is 30 days unless adjusted when entering the plate. Leaving a stale BOLO in a dispatch hotlist, which could result in a broadcast to Troopers when the vehicle is no longer wanted or sought, is a situation we seek to avoid.

Example 1: a BOLO is put out for a vehicle involved in a shooting in Springfield. This matter will be investigated by Springfield PD, and they have access to the LPR system or can contact CFC/CWC directly to use it in their investigation. The active life of this BOLO is probably not more than a few hours or end of the working crew's shift, unless circumstances dictate otherwise.

Information changes quickly, and it is the responsibility (by policy) of the members entering or requesting the entries to remove them when no longer needed. It is not the duty of our dispatchers to stay abreast of ongoing investigations. Since they may be unaware if a plate needs to stay on the hotlist, it follows that they generally should not be requesting hotlist entries for an extended period of time.

Example 2: Brockton PD broadcasts info on a recently stolen vehicle. This vehicle hasn't yet been entered into NCIC. The active life of this BOLO is also probably not more than a few hours or end of the working crew's shift. The vehicle will be entered into NCIC (and removed by the ORI when no

longer stolen). Manual hotlist entries are not intended to serve as a long term means to identify and broadcast motor vehicle offenses over troop radios.

Please let know your thoughts on this, including any other common scenarios you find when field inquiries from dispatch. Once we get the appropriate guidelines here, we can push it out to your team and to the dispatchers in their training.

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

Subject: FW: Idi Investigative Platform
Date: Thursday, June 2, 2022 2:35:39 PM
Attachments: image001.png
LawEnforcementFusionCenter_CaseStudy.pdf
idiCORE.pdf

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Thursday, June 2, 2022 11:35 AM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Cc: Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Subject: Re: Idi Investigative Platform

Good Morning!

I saw that Justin had forwarded this while I was going catching up to speed on last night. I was actually able to test idiCORE as part of a trial a few years back. It's very similar to CLEAR/TLO (and presumably Accurint/LexisNexus), and if memory serves, the company was actually started by persons who worked on TLO.

The database was pretty new when we tested it, but it did seem pretty good, especially with phone numbers, which seems to be the crux of their pitch.

Sgt. Noah Pack, who is now the ALPR Coordinator, was actually the one who I believe spearheaded the Department's trial, if anyone has any questions about it or was interested in looking into it further.

Respectfully,

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

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

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Wednesday, June 1, 2022 4:29 PM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: Fw: Idi Investigative Platform

Elly,

I am not familiar with this product. Just sending it along as an FYI.

Respectfully,

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

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

From: Omari Moench <omoench@ididata.com>
Sent: Wednesday, June 1, 2022 3:29 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Idi Investigative Platform

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.

Marci,

Great speaking with you.

I'd like to extend an invitation to a **free 30-day pilot** of our investigative platform. With unlimited users & unlimited searches

We are a 100% cloud native platform, with some of the most accurate phone numbers, criminal information & addresses.

Either way our job only works by making yours easier and with this platform I truly believe we can help close some pending cases at a higher rate with the data we are able to provide for law enforcement and FC's

Thank you for your time & service.

Looking forward to hearing from you.



Omari Moench | Account Executive
IDI, a red violet company (NASDAQ: RDVT)
2650 N. Military Trail, Suite 300
Boca Raton, FL 33431
561-757-4592 Direct
855-842-1410 Toll Free
561-336-0025 Fax
www.ididata.com

From: THEOBALD, KENT (TROOPERS)
To: Pack, Noah (POL); mark.cyr@state.ma.u
Cc: FIET, EVAN (TROOPERS)
Subject: FW: Interagency Coordination Agreement
Date: Thursday, January 20, 2022 9:03:01 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.

Major Cyr, Sgt Pack;

Good morning, NYSIC Command has authorized sharing of our LPR data with designated personnel from your agency. Please provide an MOU or other pertinent documentation concerning the sharing of information going forward.

Thank-you,

KT

Kent Theobald
Senior Investigator
New York State Police
Criminal Intelligence Unit – NYSIC
31 Tech Valley Drive
East Greenbush, NY 12061
518-786-2140

-------- Original Message --------
From: "Cyr, Mark (POL)" <mark.cyr@state.ma.us>
Date: Tue, Jan 11, 2022, 3:43 PM
To: "Pack, Noah (POL)" <noah.pack@state.ma.us>,"THEOBALD, KENT (TROOPERS)" <Kent.Theobald@troopers.ny.gov>
CC: "Tucker, Daniel T (POL)" <daniel.t.tucker@state.ma.us>
Subject: Re: Interagency Coordination Agreement

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

Thank you Noah.

Kent, please also feel free to reach me on my cell phone- [redacted] I look forward to coordinating with you and your Department to help facilitate an interagency ALPR agreement.

Mark

Major Mark D. Cyr #2728

Massachusetts State Police

Division of Homeland Security and Preparedness

Deputy Division Commander - CIIS

978-451-3773 (office)

G.L. c. 4, sec. 7,cl. 26 (c)(privacy) *(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: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 11, 2022 3:35 PM
To: kent.theobald@troopers.ny.gov <kent.theobald@troopers.ny.gov>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Interagency Coordination Agreement

Senior Investigator Theobald,

In the interest of public safety and intelligence sharing, we are interested in coordinating with NYSIC regarding interagency sharing of ALPR systems for official and lawful purposes. Specifically, we respectfully request that NYSIC grant ALPR system access to the Commonwealth Fusion Center (CFC). Reciprocally, CFC would offer access to the MSP ALPR system to NYSIC. This agreement would benefit both agencies by allowing for the timely and efficient searching and sharing of information in critical incidents and investigations and by reducing the workload placed upon each agency's fusion center staff.

For further coordination, Major Mark D. Cyr of the Division of Homeland Security and Preparedness will be the command level point-of-contact for our agency. He can be reached at 978-451-3773 or via email at mark.cyr@pol.state.ma.us, and he is Cc'd on this message. Please advise if we should contact anyone else directly within your agency.

Thank you for your assistance, and we look forward to working with you.

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
Office: 508-988-7311
Cell: 413-[redacted]

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

From: THEOBALD, KENT (TROOPERS)
To: Cyr, Mark (POL)
Subject: FW: Interagency Coordination Agreement
Date: Thursday, January 20, 2022 9:03:56 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.

Major Cyr, Sgt Pack;

Good morning, NYSIC Command has authorized sharing of our LPR data with designated personnel from your agency. Please provide an MOU or other pertinent documentation concerning the sharing of information going forward.

Thank-you,

KT

Kent Theobald
Senior Investigator
New York State Police
Criminal Intelligence Unit – NYSIC
31 Tech Valley Drive
East Greenbush, NY 12061
518-786-2140

------- Original Message --------
From: "Cyr, Mark (POL)" <mark.cyr@state.ma.us>
Date: Tue, Jan 11, 2022, 3:43 PM
To: "Pack, Noah (POL)" <noah.pack@state.ma.us>,"THEOBALD, KENT (TROOPERS)" <Kent.Theobald@troopers.ny.gov>
CC: "Tucker, Daniel T (POL)" <daniel.t.tucker@state.ma.us>
Subject: Re: Interagency Coordination Agreement

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

Thank you Noah.

Kent, please also feel free to reach me on my cell phone- 508-[redacted] I look forward to coordinating with you and your Department to help facilitate an interagency ALPR agreement.

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: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 11, 2022 3:35 PM
To: kent.theobald@troopers.ny.gov <kent.theobald@troopers.ny.gov>
Cc: Cyr, Mark (POL) <mark.cyr@pol.state.ma.us>
Subject: Interagency Coordination Agreement

Senior Investigator Theobald,

In the interest of public safety and intelligence sharing, we are interested in coordinating with NYSIC regarding interagency sharing of ALPR systems for official and lawful purposes. Specifically, we respectfully request that NYSIC grant ALPR system access to the Commonwealth Fusion Center (CFC). Reciprocally, CFC would offer access to the MSP ALPR system to NYSIC. This agreement would benefit both agencies by allowing for the timely and efficient searching and sharing of information in critical incidents and investigations and by reducing the workload placed upon each agency's fusion center staff.

For further coordination, Major Mark D. Cyr of the Division of Homeland Security and Preparedness will be the command level point-of-contact for our agency. He can be reached at 978-451-3773 or via email at mark.cyr@pol.state.ma.us, and he is Cc'd on this message. Please advise if we should contact anyone else directly within your agency.

Thank you for your assistance, and we look forward to working with you.

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
Office: 508-988-7311
Cell: 413-[redacted]

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

From: Manning, David (POL)
To: Deas, James (POL)
Cc: Crouse, David (POL); Mcnamara, Sean (POL)
Subject: Fw: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)
Date: Wednesday, August 3, 2022 9:18:43 AM
Attachments: image001.png
NexusClient QRG 7.2.0 202112021640.pdf
Nexus Mobile QRG 202006171029.pdf
Copy of NEW EMS System Admin 7.2.0 202111301641.pdf

Trooper David M. Manning
Massachusetts State Police
Division of Homeland Security and Preparedness
Technical Services Unit

Cell: 617[redacted]

From: Dave M <2016645@gmail.com>
Sent: Wednesday, August 3, 2022 9:15 AM
To: Manning, David (POL) <david.manning@pol.state.ma.us>
Subject: Fwd: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

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.

Sent from my iPhone

Begin forwarded message:

> **From:** Paul Allen <paul@airshipvms.com>
> **Date:** August 3, 2022 at 07:59:35 EDT
> **To:** Dave Manning <2016645@gmail.com>
> **Cc:** bob.fecteau@outlook.com, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com
> **Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)**
>
> Dave, see attached download link, was just about to hit send. If you want to download this file to the desktop we can walk through the rest of it when we do the setup. Also, if you want to download our Mobile App on your iPhone or Android pull that down in advance and we can go through the setup then. The app is called Nexus Mobile on either store / marketplace with the icon being the orange airship on a black

background. Also attached to this email are the user guides for EMS and the various client applications for further review if you have questions after we get everything up and running. Look forward to the discussion later today.

https://fetch.airshipvms.com/Airship_x64_8.0.0.81_AIO_Install.exe

v/r

Paul

AIRSHIP
Paul Allen
President
AIRSHIP Industries, Inc.,
12226 134th CT NE
Redmond, WA 98052
704.798.7973

The information contained in this transmission is confidential and/or may contain client privileged communications intended for the use of the individual or entity named above, and JDL Digital Systems (DBA Airship Industries, Inc.). If the reader of this electronic message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying is strictly prohibited.

From: Dave Manning <2016645@gmail.com>
Date: Wednesday, August 3, 2022 at 7:49 AM
To: paul@airshipvms.com <paul@airshipvms.com>
Cc: bob.fecteau@outlook.com <bob.fecteau@outlook.com>, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com <tyler@airshipvms.com>
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Thanks Paul. You mentioned previously that you would send a download link to save time. Is that something you still want to do, or shall we wait until our Zoom?

Dave

On Tue, Aug 2, 2022 at 9:34 PM <paul@airshipvms.com> wrote:

Paul Allen is inviting you to a scheduled Zoom meeting.
Join Zoom Meeting
https://us06web.zoom.us/j/84554805559?pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
Meeting ID: 845 5480 5559
Passcode: 757394
One tap mobile
+13126266799,,84554805559#,,,,*757394# US (Chicago)
+16469313860,,84554805559#,,,,*757394# US
Dial by your location
+1 312 626 6799 US (Chicago)
+1 646 931 3860 US
+1 929 436 2866 US (New York)
+1 301 715 8592 US (Washington DC)
+1 669 900 6833 US (San Jose)
+1 253 215 8782 US (Tacoma)
+1 346 248 7799 US (Houston)
+1 386 347 5053 US
+1 564 217 2000 US
+1 669 444 9171 US
Meeting ID: 845 5480 5559
Passcode: 757394
Find your local number: https://us06web.zoom.us/u/kMEG8yJaM

When

Wednesday Aug 3, 2022 · 12pm – 1pm (Eastern Time - New York)

Location

https://us06web.zoom.us/j/84554805559?pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
View map

Guests

paul@airshipvms.com - organizer
2016645@gmail.com
bob.fecteau@outlook.com
Dominic Splattstoesser
tyler@airshipvms.com
View all guest info

Reply for 2016645@gmail.com

Yes | No | Maybe

More options

Invitation from Google Calendar
You are receiving this email because you are subscribed to calendar notifications. To stop receiving these emails, go to Calendar settings, select this calendar, and change "Other notifications".
Forwarding this invitation could allow any recipient to send a response to the organizer, be added to the guest list, invite others regardless of their own invitation status, or modify your RSVP. Learn more

From: Reich, LisaAnn (CJT)
To: Reich, LisaAnn (CJT)
Subject: FW: legal update - new rule for search warrants for CSLI tower dumps
Date: Thursday, April 14, 2022 6:50:42 PM
Attachments: perry.pdf
legal update - new rule for search warrants for CSLI tower dumps.pdf

---

FYI - LAR

From: Flagg, Denise S. (CJT) <Denise.S.Flagg@mass.gov>
Sent: Thursday, April 14, 2022 4:53 PM

Subject: legal update - new rule for search warrants for CSLI tower dumps

Good afternoon.

Attached please find a legal update that was sent out this afternoon to all MPTC instructors and department training coordinators. The legal update is regarding the recent SJC decision Commonwealth v. Perry. In this case the court reviews two search warrants for tower dumps for CSLI data that were obtained to identify the perpetrator of six robberies and an attempted robbery that resulted in homicide. The court also announces a new rule with respect to search warrants for tower dumps. In the future, only a judge can issue a search warrant for tower dumps. In addition, the warrant must include protocols for the prompt and permanent disposal of data collected that does not fit within the object of the search. A copy of the case is attached to this email.

Please let me know if you have any questions.

Denise

Denise S. Flagg, Esq.
Legal Issues Coordinator
Municipal Police Training Committee
42 Thomas Patten Drive
Randolph, MA 02368
(781) 437-0319

The preceding email message, including attachments, contains information that may be protected by attorney/client or other applicable privilege or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not the intended recipient of this email, please notify the sender by replying to this email and then delete all copies of it from your computer system. Any use, dissemination, reproduction or distribution of this email and its contents to unintended recipients is not unauthorized and may be unlawful.

From: Grant, Timothy (DAC)
To: Pham, Cynthia H. (DAC); Connor, Joseph (DAC); Joyal, Benjamin (DAC); Mungovan, Katherine (DAC)
Subject: FW: legal update - new rule for search warrants for CSLI tower dumps
Date: Friday, April 15, 2022 4:35:53 PM
Attachments: perry.pdf
legal update - new rule for search warrants for CSLI tower dumps.pdf

---

FYI

From: Denise S Flagg <no-reply@acadisonline.com>
Sent: Thursday, April 14, 2022 4:51 PM
To: Grant, Timothy (DAC) <timothy.grant@mass.gov>
Subject: legal update - new rule for search warrants for CSLI tower dumps

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.

Attached please find a legal update regarding the recent SJC decision Commonwealth v. Perry. In this case the court reviews two search warrants for tower dumps for CSLI data that were obtained to identify the perpetrator of six robberies and an attempted robbery that resulted in homicide. The court also announces a new rule with respect to search warrants for tower dumps. In the future, only a judge can issue a search warrant for tower dumps. In addition, the warrant must include protocols for the prompt and permanent disposal of data collected that does not fit within the object of the search. A copy of the case is attached to this email.

Please let me know if you have any questions.

Denise

Denise S. Flagg, Esq.
Legal Issues Coordinator
Municipal Police Training Committee
42 Thomas Patten Drive
Randolph, MA 02368
(781) 437-0319

The preceding email message, including attachments, contains information that may be protected by attorney/client or other applicable privilege or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not the intended recipient of this email, please notify the sender by replying to this email and then delete all copies of it from your computer system. Any use, dissemination, reproduction or distribution of this email and its contents to unintended recipients is not unauthorized and may be unlawful.

Subject: FW: MA State Police Dispatch Services Unit: FLOCK
Date: Thursday, January 27, 2022 7:31:52 AM
Attachments: 2020 COMSEC Annual Report.docx
Flock LPR To-From 01-26-2022.pdf
1_LPR.pdf
2_LPR.pdf
3a_LPR.pdf
3b_LPR.pdf
4_LPR.pdf

Matt,

Attached are several documents re: LPR:

- Some email dating back to December 2020 after 3M/BOSS was paused, including an email exchange with Jen Staples about the issue.
- Some emails regarding a LPR audit I did in December 2021.
- The 2020 COMSEC Annual Report that includes mention that we were using FLOCK on a limited basis at AHQ.

Also,

- The to/from by Mike Slater with the information you requested.
- Still waiting on a response from Pete Cheverie, but he is working on the document,

Respectfully,
Ken

_____

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 222
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Barstow, Matthew (POL) <matthew.barstow@pol.state.ma.us>
Sent: Tuesday, January 25, 2022 5:36 PM
To: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>
Subject: Fwd: MA State Police Dispatch Services Unit: FLOCK

I assume you are aware of this and asked Pete to reach out to Lynn?

With the sensitivity of LPRs and their relationship to privacy, I imagine Colonel is going to direct that these kinds of agreements get vetted through Legal, or at least at a higher level then just a DIII at a

center.

Matthew C. Barstow
Director of Telecommunications
MA State Police Headquarters
470 Worcester Rd
Framingham, MA 01702
Tel (508) 820-2264
Fax (508) 820-2359
matthew.barstow@mass.gov
————————————————

Begin forwarded message:

> **From:** "Wilcox, Christopher (POL)" <christopher.wilcox@pol.state.ma.us>
> **Date:** January 25, 2022 at 17:26:54 EST
> **To:** "Barstow, Matthew (POL)" <matthew.barstow@pol.state.ma.us>
> **Subject: Fwd: MA State Police Dispatch Services Unit: FLOCK**
>
> Matt. Can we talk about this tomorrow
>
> LTC Chris Wilcox
> Division of Homeland Security and Preparedness
>
> Begin forwarded message:
>
> > **From:** "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>
> > **Date:** January 25, 2022 at 4:13:36 PM EST
> > **To:** "Wilcox, Christopher (POL)" <christopher.wilcox@pol.state.ma.us>
> > **Subject: Fwd: MA State Police Dispatch Services Unit: FLOCK**
> >
> > Sir, FYI I just received this today.
> >
> > 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:** O'Toole, Mark <otoole@lynnpolice.org>
> > **Sent:** Tuesday, January 25, 2022 16:01

From: Cheverie, Peter (POL) [mailto:peter.cheverie@state.ma.us]
Sent: Wednesday, December 29, 2021 11:17 AM
To: O'Toole, Mark <otoole@lynnpolice.org>
Subject: MA State Police Dispatch Services Unit: FLOCK

Hi Captain O'Toole,

My name is Pete Cheverie, I run the MA State Police Troop A Dispatch Services Unit, located at our Danvers Headquarters. One of my dispatchers, Gary Ferguson, advised me of your conversations about the FLOCK LPR System and the user account you have set up for MSP. I wanted to thank you for your willingness to make this available to us; as we have had great success with Chelsea's Flock LPR system as well.

Before I authorize my team to access your account, I just have to confirm with you that in the interest of public safety, the Lynn Police Department is voluntarily granting MSP access an authorized user on your system. The MSP cannot currently commit to any financial responsibility or future reimbursement to the City of Lynn as a guest user of this resource. Additionally, the MSP cannot take on any primary responsibility for monitoring any alerts, BOLO's, or other notifications as designed by the Flock System. If you are okay with this, the MSP greatly appreciates your time and look forward to assisting your department in proving how useful Flock can be for your city.

Please reach out any time with any questions or concerns.

Respectfully,

Pete

Peter J. Cheverie, CMCP | Center Supervisor
Massachusetts State Police
Dispatch Services Unit
Troop "A" Headquarters
485 Maple Street
Danvers, MA 01923
tel: 978.538.6113 | fax: 978.538.6185
Peter.Cheverie@mass.gov | http://www.mass.gov/msp

Confidentiality Notice:
THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly

prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Handfield, Kenneth (POL)
To: Barstow, Matthew (POL)
Subject: FW: MA State Police Dispatch Services Unit: FLOCK
Date: Thursday, January 27, 2022 7:32:36 AM
Attachments: 2020 COMSEC Annual Report.docx
Flock LPR To-From 01-26-2022.pdf
1_LPR.pdf
2_LPR.pdf
3a_LPR.pdf
3b_LPR.pdf
4_LPR.pdf

Matt,

Attached are several documents re: LPR:

- Some email dating back to December 2020 after 3M/BOSS was paused, including an email exchange with Jen Staples about the issue.
- Some emails regarding a LPR audit I did in December 2021.
- The 2020 COMSEC Annual Report that includes mention that we were using FLOCK on a limited basis at AHQ.

Also,

- The to/from by Mike Slater with the information you requested.
- Still waiting on a response from Pete Cheverie, but I have confirmed he is working on the document,

Respectfully,
Ken

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 222
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Barstow, Matthew (POL) <matthew.barstow@pol.state.ma.us>
Sent: Tuesday, January 25, 2022 5:36 PM
To: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>
Subject: Fwd: MA State Police Dispatch Services Unit: FLOCK

I assume you are aware of this and asked Pete to reach out to Lynn?

With the sensitivity of LPRs and their relationship to privacy, I imagine Colonel is going to direct that these kinds of agreements get vetted through Legal, or at least at a higher level then just a DIII at a center.

Matthew C. Barstow
Director of Telecommunications
MA State Police Headquarters
470 Worcester Rd
Framingham, MA 01702
Tel (508) 820-2264
Fax (508) 820-2359
matthew.barstow@mass.gov
————————————————

Begin forwarded message:

> **From:** "Wilcox, Christopher (POL)" <christopher.wilcox@pol.state.ma.us>
> **Date:** January 25, 2022 at 17:26:54 EST
> **To:** "Barstow, Matthew (POL)" <matthew.barstow@pol.state.ma.us>
> **Subject: Fwd: MA State Police Dispatch Services Unit: FLOCK**
>
> Matt. Can we talk about this tomorrow
>
> LTC Chris Wilcox
> Division of Homeland Security and Preparedness
>
> Begin forwarded message:
>
> > **From:** "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>
> > **Date:** January 25, 2022 at 4:13:36 PM EST
> > **To:** "Wilcox, Christopher (POL)" <christopher.wilcox@pol.state.ma.us>
> > **Subject: Fwd: MA State Police Dispatch Services Unit: FLOCK**
> >
> > Sir, FYI I just received this today.
> >
> > 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:** O'Toole, Mark <otoole@lynnpolice.org>

Sent: Tuesday, January 25, 2022 16:01

From: Cheverie, Peter (POL) [mailto:peter.cheverie@state.ma.us]
Sent: Wednesday, December 29, 2021 11:17 AM
To: O'Toole, Mark <otoole@lynnpolice.org>
Subject: MA State Police Dispatch Services Unit: FLOCK

Hi Captain O'Toole,

My name is Pete Cheverie, I run the MA State Police Troop A Dispatch Services Unit, located at our Danvers Headquarters. One of my dispatchers, Gary Ferguson, advised me of your conversations about the FLOCK LPR System and the user account you have set up for MSP. I wanted to thank you for your willingness to make this available to us; as we have had great success with Chelsea's Flock LPR system as well.

Before I authorize my team to access your account, I just have to confirm with you that in the interest of public safety, the Lynn Police Department is voluntarily granting MSP access an authorized user on your system. The MSP cannot currently commit to any financial responsibility or future reimbursement to the City of Lynn as a guest user of this resource. Additionally, the MSP cannot take on any primary responsibility for monitoring any alerts, BOLO's, or other notifications as designed by the Flock System. If you are okay with this, the MSP greatly appreciates your time and look forward to assisting your department in proving how useful Flock can be for your city.

Please reach out any time with any questions or concerns.

Respectfully,

Pete

Peter J. Cheverie, CMCP | Center Supervisor
Massachusetts State Police
Dispatch Services Unit
Troop "A" Headquarters
485 Maple Street
Danvers, MA 01923
tel: 978.538.6113 | fax: 978.538.6185
Peter.Cheverie@mass.gov | http://www mass.gov/msp

Confidentiality Notice:
THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is

covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL)
To: Sullivan, Margaret (POL)
Subject: FW: MASP Connected Cruiser Solution - FirstNet
Date: Wednesday, January 26, 2022 10:42:54 AM
Attachments: wgd00000_a_4re_lte_upload_guide.pdf
wgd00085_4re_vehicle_installation_instructions.pdf

FYI

From: Egnitz, Brian (POL)
To: Connor, Debora (POL)
Subject: FW: MASP Connected Cruiser Solution - FirstNet
Date: Wednesday, January 26, 2022 10:29:30 AM
Attachments: wgd00000_a_4re_lte_upload_guide.pdf
wgd00085_4re_vehicle_installation_instructions.pdf

From: Egnitz, Brian (POL)
Sent: Wednesday, January 26, 2022 10:18 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Mitchell, Timothy P. (EOTSS) <Timothy.P.Mitchell@mass.gov>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: FW: MASP Connected Cruiser Solution - FirstNet

FYI

From: Egnitz, Brian (POL)
To: Guerriero, Robert (EOTSS); Mitchell, Timothy P. (EOTSS)
Cc: Driscoll, Francis (POL)
Subject: FW: MASP Connected Cruiser Solution - FirstNet
Date: Wednesday, January 26, 2022 10:18:24 AM
Attachments: wgd00000_a_4re_lte_upload_guide.pdf
wgd00085_4re_vehicle_installation_instructions.pdf

FYI

From: Sullivan, Margaret (POL)
To: Kelly, Edward (POL)
Subject: FW: MASP Connected Cruiser Solution - FirstNet
Date: Wednesday, January 26, 2022 11:50:00 AM
Attachments: wgd00000_a_4re_lte_upload_guide.pdf
wgd00085_4re_vehicle_installation_instructions.pdf

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, January 26, 2022 10:43 AM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Subject: FW: MASP Connected Cruiser Solution - FirstNet

FYI

From: Biagi, Pamela (POL)
To: Comeau, Melissa (POL)
Cc: Silva, Kyra (POL)
Subject: FW: mass DOT question
Date: Monday, January 24, 2022 3:34:57 PM
Attachments: image001.png
SCF_MSP_BainCor_executed.pdf
massDOT_telecom_RFR.pdf
Award - Bain Cor AW.pdf

Just an FYI

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Thursday, January 20, 2022 10:19 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rossi, Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE: massDOT question

Good morning Sgt. Pack,

The MSP-BainCor Inc. contract has been signed by both parties and is fully executed. I will send Mr. Bainter a copy for his file.

Looping in Pamela Biagi, Director of Fiscal Services.

Pam: this is a "piggyback" contract through MassDOT for a purchase of ALPR solar trailers. Also attached is the MassDOT contract for information purposes.

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:27 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. We hope to be purchasing solar trailers from Baincor.

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:25 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: RE: massDOT question

Hi SGT Pack,

I will send out the SCF to Wayne Bainter at BainCor, Inc. I will cc you.

I apologize, can you refresh my memory? What is MSP purchasing from Baincor?

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:15 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. I will let our contact at Baincor know. Is there anything I can do to facilitate that contract execution?

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:13 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: FW: massDOT question

Hi Sgt. Pack,

Good news. As I mentioned, I hadn't heard back from John Polcari over at MassDOT, but a contact I have over there got back to me almost immediately. Please see below. MSP has been approved to utilize the MassDOT contract with Baincor under sperate contract execution. MassDOT is going to send me a copy of the contract packet for our procurement file.

The last step will be for MSP to have an authorized signatory form Baincor sign a Standard Contract Form (SCF) and send it back to me for CAO Small's signature. I will have an SCF sent to the contract person at Baincor and keep you posted.

Thank you,
Brian

From: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday, January 18, 2022 1:48 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE: massDOT question

Hi Brian,

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it's open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet, which will include the executed SCF. Once I receive it, I will pass it along to you.

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 1:38 PM
To: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John,

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn't heard. Please see

the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Biagi, Pamela (POL)
To: Comeau, Mel ssa (POL)
Subject: FW: massDOT quest on
Date: Wednesday, January 26, 2022 12:33:00 PM
Attachments: SCF_MSP_Ba nCor_executed.pdf
MBPO 24335.PDF
2020_MAR_Telecomm_RFR_F nal-Rev sed-July docx
image001.png
image002.png

FYI in case you need this contract.

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Wednesday January 26 2022 12 15 PM
To: Biagi Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Cc: Silva Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: FW massDOT question

Hi Pam

FYI. This is a "piggyback" contract through MassDOT. Division of Homeland Security was hoping to use BainCor to purchase ALPR solar trailers.

MassDOT added us to their MA. Dianne included the MA number below.

As for the MBPO MassDOT does not create MBPO s in COMMBUYS currently. Only bid solicitations. Therefore Dianne did a direct PO to the vendor in this case referencing the MassDOT contract. Number below/attached.

Thank you
Brian

From: Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 57 AM
To: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>
Cc: Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian
I wasn t sure who the purchasing info would go to.

MMARS MA DOT INFT0000K03C00111753
COMMBUYS MBPO PO-22-1084-POLGH-GHQ-24335

Expires 6/30/2025

From: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>
Sent: Wednesday January 26 2022 11 06 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>; Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Thank you everyone for the assistance. It is much appreciated.

Sincerely

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 59 AM
To: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John D Bianchi@dot state ma us>; Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>; Miller Dianne (POL) <Dianne Miller@pol state ma us>
Subject: RE massDOT question

Hi Dan

Department of State Police (POL) has bee added to MA INTF0000K03C00111753 version 10 and is now final.

Mary Mariani
Accountant III
MassDOT
10 Park Plaza, Ste 5450
Boston, MA 02116
mary.mariani@state.ma.us
(P) 857-368-9068
(F) 857-368-0637

From: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 25 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Mary – can you please add POL as an authorized Department for MA DOT INTF0000K03C00111753 and let everyone on this e-mail know when it has been put to Final in MMARS.

Thank You!

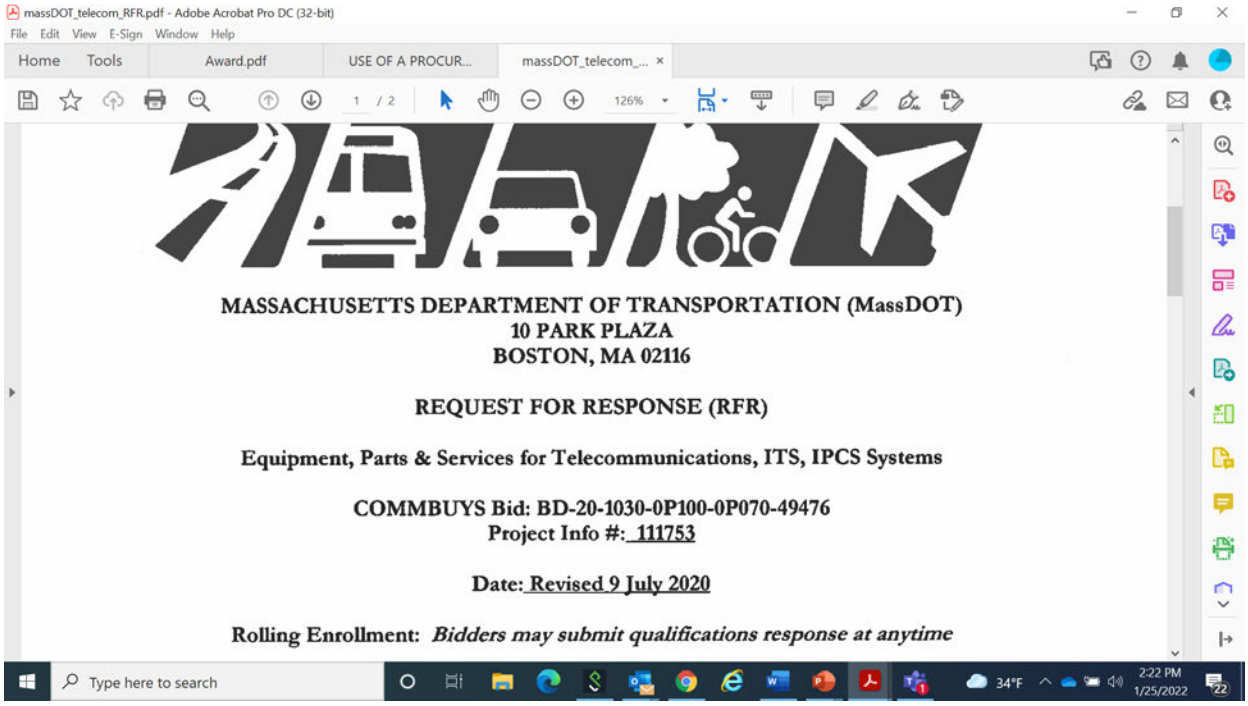
Daniel Lee
Deputy Director of Accounting
10 Park Plaza – Suite 5510
Boston, MA 02116
Phone: (857)-368-9074
Work M.G.L. c. 4, sec. 7 cl. 26 (c)

From: Bianchi John D. (DOT) <John D Bianchi@dot state ma us>
Sent: Tuesday January 25 2022 2 27 PM
To: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Hi Dan

I have granted POL permission to access the contract you see below. Can you please confirm if there is a MA for this and if there is can you please add POL as an authorized user and share the MA # with our friends from POL cc d here?

Thank you Dan.



From: Bianchi John D. (DOT)
Sent: Tuesday January 18 2022 1 48 PM
To: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>
Subject: RE massDOT question

Hi Brian

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it s open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet which will include the executed SCF. Once I receive it I will pass it along to you.

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday January 18 2022 1 38 PM
To: Bianchi John D. (DOT) <John D Bianchi@dot state ma us>
Subject: massDOT question

Hi John

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn t heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police

470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Kearnan, Brian J. (POL)
To: Biagi, Pamela (POL)
Cc: Silva, Kyra (POL); Miller, Dianne (POL); Rossi, Gina (POL)
Subject: FW: massDOT quest on
Date: Wednesday, January 26, 2022 12:15:14 PM
Attachments: SCF_MSP_Ba nCor_executed.pdf
MBPO 24335.PDF
2020_MAR_Telecomm_RFR_F nal-Rev sed-July docx
image001.png
image002.png

Hi Pam

FYI. This is a "piggyback" contract through MassDOT. Division of Homeland Security was hoping to use BainCor to purchase ALPR solar trailers.

MassDOT added us to their MA. Dianne included the MA number below.

As for the MBPO MassDOT does not create MBPO s in COMMBUYS currently. Only bid solicitations. Therefore Dianne did a direct PO to the vendor in this case referencing the MassDOT contract. Number below/attached.

Thank you
Brian

From: Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 57 AM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian
I wasn t sure who the purchasing info would go to.

MMARS MA DOT INFT0000K03C00111753
COMMBUYS MBPO PO-22-1084-POLGH-GHQ-24335

Expires 6/30/2025

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 06 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>; Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Thank you everyone for the assistance. It is much appreciated.

Sincerely

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 59 AM
To: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Hi Dan

Department of State Police (POL) has bee added to MA INTF0000K03C00111753 version 10 and is now final.

Mary Mariani
Accountant III
MassDOT
10 Park Plaza, Ste 5450
Boston, MA 02116
mary.mariani@state.ma.us
(P) 857-368-9068
(F) 857-368-0637

From: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 25 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Mary – can you please add POL as an authorized Department for MA DOT INTF0000K03C00111753 and let everyone on this e-mail know when it has been put to Final in MMARS.

Thank You!

Daniel Lee
Deputy Director of Accounting
10 Park Plaza – Suite 5510

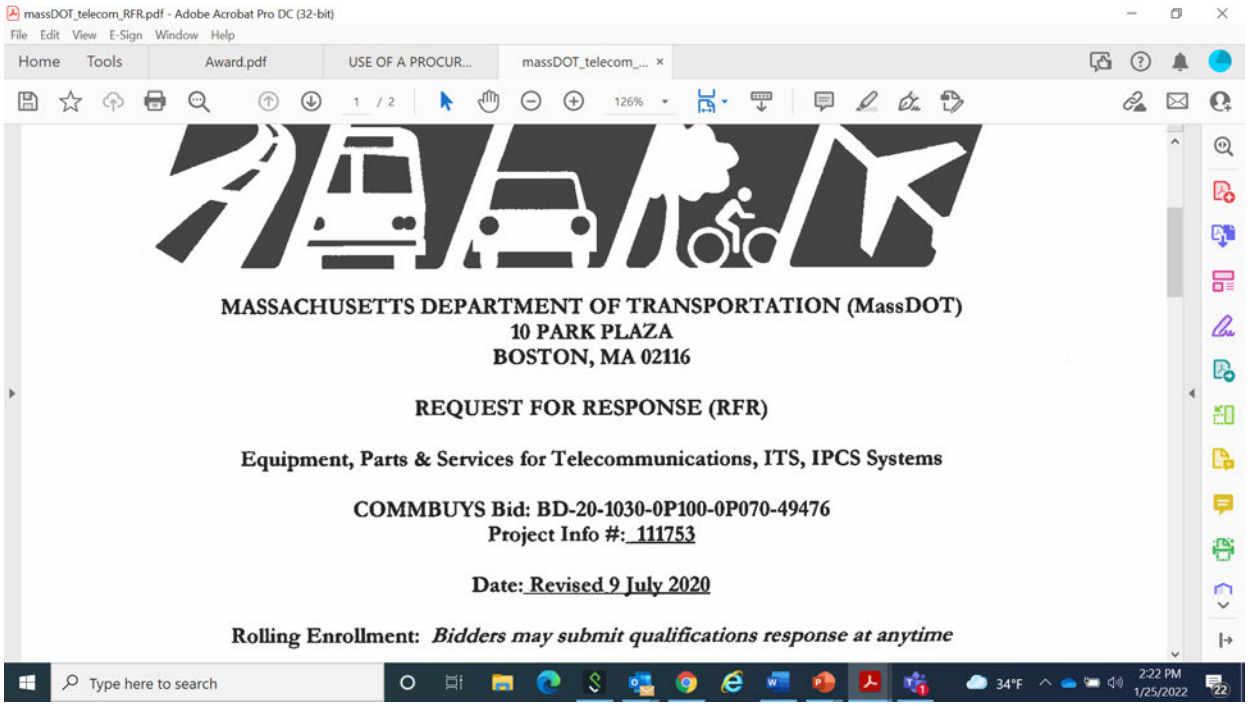
Boston, MA 02116
Phone: (857)-368-9074
Work Cell [redacted]

From: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday January 25 2022 2 27 PM
To: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>; Miller Dianne (POL) <Dianne Miller@pol state ma us>
Subject: FW massDOT question

Hi Dan

I have granted POL permission to access the contract you see below. Can you please confirm if there is a MA for this and if there is can you please add POL as an authorized user and share the MA # with our friends from POL cc d here?

Thank you Dan.



From: Bianchi John D. (DOT)
Sent: Tuesday January 18 2022 1 48 PM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it s open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet which will include the executed SCF. Once I receive it I will pass it along to you.

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday January 18 2022 1 38 PM
To: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn t heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us


MASSACHUSETTS
STATE
POLICE

To: Biagi, Pamela (POL)
Cc: Silva, Kyra (POL); Miller, Dianne (POL); Rossi, Gina (POL)
Subject: FW: massDOT quest on
Date: Wednesday, January 26, 2022 12:13:01 PM
Attachments: SCF_MSP_Ba nCor_executed.pdf
MBPO 24335.PDF
2020_MAR_Telecomm_RFR_F nal-Revised-July.docx
mage001.png
mage002.png

Hi Pam

FYI. This is a "piggyback" contract through MassDOT. Homeland Security was looking to use BainCor to purchase ALPR solar trailers.

MassDOT added us to their MA. Dianne included the MA number below.

As for the MBPO MassDOT does not create MBPO s in COMMBUYS currently. Only bid solicitations. Therefore Dianne did a direct PO to the vendor in this case referencing the MassDOT contract. Number below/attached.

Thank you
Brian

From: Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 57 AM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian
I wasn t sure who the purchasing info would go to.

MMARS MA DOT INFT0000K03C00111753
COMMBUYS MBPO PO-22-1084-POLGH-GHQ-24335

Expires 6/30/2025

From: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>
Sent: Wednesday January 26 2022 11 06 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>; Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Thank you everyone for the assistance. It is much appreciated.

Sincerely

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 59 AM
To: Lee Daniel (DOT) <Daniel Lee@dot state ma us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Hi Dan

Department of State Police (POL) has bee added to MA INTF0000K03C00111753 version 10 and is now final.

Mary Mariani
Accountant III
MassDOT
10 Park Plaza, Ste 5450
Boston, MA 02116
mary.mariani@state.ma.us
(P) 857-368-9068
(F) 857-368-0637

From: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 25 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Mary – can you please add POL as an authorized Department for MA DOT INTF0000K03C00111753 and let everyone on this e-mail know when it has been put to Final in MMARS.

Thank You!

Daniel Lee
Deputy Director of Accounting
10 Park Plaza – Suite 5510
Boston, MA 02116

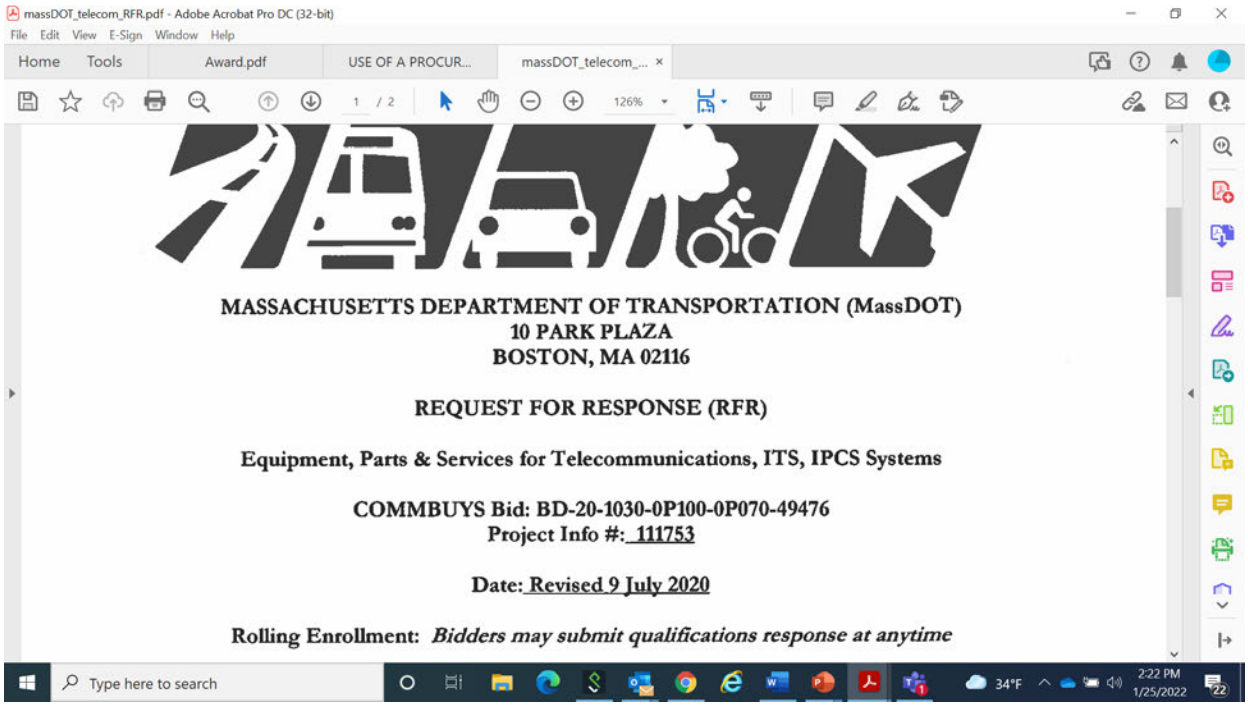
Phone: (857)-368-9074
Work Cell: (617) [redacted]

From: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday January 25 2022 2 27 PM
To: Lee Daniel (DOT) <Daniel Lee@dot state ma us>
Cc: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Hi Dan

I have granted POL permission to access the contract you see below. Can you please confirm if there is a MA for this and if there is can you please add POL as an authorized user and share the MA # with our friends from POL cc d here?

Thank you Dan.



From: Bianchi John D. (DOT)
Sent: Tuesday January 18 2022 1 48 PM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it s open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet which will include the executed SCF. Once I receive it I will pass it along to you.

From: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>
Sent: Tuesday January 18 2022 1 38 PM
To: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn t heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us


MASSACHUSETTS
STATE
POLICE

To: Comeau, Melissa (POL)
Cc: Silva, Kyra (POL)
Subject: FW: massDOT question
Date: Thursday, January 20, 2022 10:40:17 AM
Attachments: image001.png
SCF_MSP_BainCor_executed.pdf
massDOT_telecom_RFR.pdf
Award - Bain Cor AW.pdf

Just an FYI

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Thursday, January 20, 2022 10:19 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rossi, Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE: massDOT question

Good morning Sgt. Pack,

The MSP-BainCor Inc. contract has been signed by both parties and is fully executed. I will send Mr. Bainter a copy for his file.

Looping in Pamela Biagi, Director of Fiscal Services.

Pam: this is a "piggyback" contract through MassDOT for a purchase of ALPR solar trailers. Also attached is the MassDOT contract for information purposes.

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:27 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. We hope to be purchasing solar trailers from Baincor.

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:25 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: RE: massDOT question

Hi SGT Pack,

I will send out the SCF to Wayne Bainter at BainCor, Inc. I will cc you.

I apologize, can you refresh my memory? What is MSP purchasing from Baincor?

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:15 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. I will let our contact at Baincor know. Is there anything I can do to facilitate that contract execution?

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>

Sent: Tuesday, January 18, 2022 2:13 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: FW: massDOT question

Hi Sgt. Pack,

Good news. As I mentioned, I hadn't heard back from John Polcari over at MassDOT, but a contact I have over there got back to me almost immediately. Please see below. MSP has been approved to utilize the MassDOT contract with Baincor under sperate contract execution. MassDOT is going to send me a copy of the contract packet for our procurement file.

The last step will be for MSP to have an authorized signatory form Baincor sign a Standard Contract Form (SCF) and send it back to me for CAO Small's signature. I will have an SCF sent to the contract person at Baincor and keep you posted.

Thank you,
Brian

From: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday, January 18, 2022 1:48 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE: massDOT question

Hi Brian,

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it's open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet, which will include the executed SCF. Once I receive it, I will pass it along to you.

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 1:38 PM
To: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John,

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn't heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check

on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Pack, Noah (POL)
To: Egnitz, Brian (POL)
Cc: Wilcox, Christopher (POL)
Subject: FW: massDOT question
Date: Thursday, January 20, 2022 10:20:00 AM
Attachments: image001.png
SCF_MSP_BainCor_executed.pdf
massDOT_telecom_RFR.pdf
Award - Bain Cor AW.pdf

Trailer contract has been completed with the vendor and can be purchased if and when Amy so chooses.

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Thursday, January 20, 2022 10:19 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Biagi, Pamela (POL) <Pamela.Biagi@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rossi, Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE: massDOT question

Good morning Sgt. Pack,

The MSP-BainCor Inc. contract has been signed by both parties and is fully executed. I will send Mr. Bainter a copy for his file.

Looping in Pamela Biagi, Director of Fiscal Services.

Pam: this is a "piggyback" contract through MassDOT for a purchase of ALPR solar trailers. Also attached is the MassDOT contract for information purposes.

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:27 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. We hope to be purchasing solar trailers from Baincor.

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:25 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: RE: massDOT question

Hi SGT Pack,

I will send out the SCF to Wayne Bainter at BainCor, Inc. I will cc you.

I apologize, can you refresh my memory? What is MSP purchasing from Baincor?

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:15 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. I will let our contact at Baincor know. Is there anything I can do to facilitate that contract execution?

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:13 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: FW: massDOT question

Hi Sgt. Pack,

Good news. As I mentioned, I hadn't heard back from John Polcari over at MassDOT, but a contact I have over there got back to me almost immediately. Please see below. MSP has been approved to utilize the MassDOT contract with Baincor under sperate contract execution. MassDOT is going to send me a copy of the contract packet for our procurement file.

The last step will be for MSP to have an authorized signatory form Baincor sign a Standard Contract Form (SCF) and send it back to me for CAO Small's signature. I will have an SCF sent to the contract person at Baincor and keep you posted.

Thank you,
Brian

From: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday, January 18, 2022 1:48 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE: massDOT question

Hi Brian,

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it's open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet, which will include the executed SCF. Once I receive it, I will pass it along to you.

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>

Sent: Tuesday, January 18, 2022 1:38 PM
To: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John,

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn't heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Biagi, Pamela (POL)
To: Clark, James (POL); Doherty, Nancy (POL); Gray, Kell e (POL); LeBlanc, Nicole (POL); Meagher, Ann (POL); Pearson, Gustav (POL); Yanoff, Benjamin (POL)
Subject: FW: massDOT quest on
Date: Wednesday, January 26, 2022 1:29:05 PM
Attachments: SCF_MSP_Ba nCor_executed.pdf
MBPO 24335.PDF
2020_MAR_Telecomm_RFR_F nal-Rev sed-July docx
image001.png
image002.png
im_ge003.png

FYI

Pamela Biagi
Director of Fiscal Services
Massachusetts State Police
470 Worcester Rd
Framingham, MA 01702
508-820-2126
Pamela Biagi@pol state ma us

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Wednesday January 26 2022 12 15 PM
To: Biagi Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Cc: Silva Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: FW massDOT question

Hi Pam

FYI. This is a "piggyback" contract through MassDOT. Division of Homeland Security was hoping to use BainCor to purchase ALPR solar trailers.

MassDOT added us to their MA. Dianne included the MA number below.

As for the MBPO MassDOT does not create MBPO s in COMMBUYS currently. Only bid solicitations. Therefore Dianne did a direct PO to the vendor in this case referencing the MassDOT contract. Number below/attached.

Thank you
Brian

From: Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 57 AM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian
I wasn t sure who the purchasing info would go to.

MMARS MA DOT INFT0000K03C00111753
COMMBUYS MBPO PO-22-1084-POLGH-GHQ-24335

Expires 6/30/2025

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 06 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>; Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Thank you everyone for the assistance. It is much appreciated.

Sincerely

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 59 AM
To: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Hi Dan

Department of State Police (POL) has bee added to MA INTF0000K03C00111753 version 10 and is now final.

Mary Mariani
Accountant III
MassDOT
10 Park Plaza, Ste 5450
Boston, MA 02116
mary.mariani@state.ma.us
(P) 857-368-9068
(F) 857-368-0637

From: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 25 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Mary – can you please add POL as an authorized Department for MA DOT INTF0000K03C00111753 and let everyone on this e-mail know when it has been put to Final in MMARS.

Thank You!

Daniel Lee
Deputy Director of Accounting
10 Park Plaza – Suite 5510
Boston, MA 02116
Phone: (857)-368-9074
Work Cell: (617) [redacted]

From: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday January 25 2022 2 27 PM
To: Lee Daniel (DOT) <Daniel Lee@dot state ma us>
Cc: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Hi Dan

I have granted POL permission to access the contract you see below. Can you please confirm if there is a MA for this and if there is can you please add POL as an authorized user and share the MA # with our friends from POL cc d here?

Thank you Dan.



From: Bianchi John D. (DOT)
Sent: Tuesday January 18 2022 1 48 PM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it s open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet which will include the executed SCF. Once I receive it I will pass it along to you.

From: Kearnan Brian J. (POL) <Brian J Kearnan@pol state ma us>
Sent: Tuesday January 18 2022 1 38 PM

To: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn t heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian J Kearnan@pol state ma us

From: Staples, Jennifer (POL)
To: Brunelli, Daniel (POL)
Subject: FW: MOU Draft
Date: Thursday, February 24, 2022 1:28:01 PM
Attachments: MOU DRAFT.docx
image001.png

Let's both take a look at this and discuss.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

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: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, February 8, 2022 3:04 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Brunelli, Daniel (POL) <Daniel.Brunelli@pol.state.ma.us>
Cc: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: MOU Draft

Attached is a draft of an MOU document that we intend to ask our local partners to sign when we switch over their ALPR equipment to our new system. Our switchover process is ongoing, so I took some time to draft this for your review and consideration. Thank you.

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

To: Breck, Kathy
Cc: jeff; Schwarz, William J; Staples, Jennifer (POL)
Subject: FW: SPD and ALPR MOU
Date: Monday, September 12, 2022 1:50:57 PM
Attachments: ALPR TENANT MOU, with SPD proposed edits.II.JMS.Edits.8.25.22.docx

---

Hello Kathy,

Revisiting the MOU discussion, after reviewing this with our Departments legal counsel, we are comfortable modifying the agreement to reflect SPD's reliance on its own policy. Attached are the proposed changes to that document. Please advise if this is acceptable to you.

Respectable,

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: Pack, Noah (POL)
To: Breck, Kathy
Cc: jeff; Schwarz, William J; Staples, Jennifer (POL)
Subject: FW: SPD and ALPR MOU
Date: Monday, September 12, 2022 1:52:00 PM
Attachments: ALPR TENANT MOU, with SPD proposed edits.II.JMS.Edits.8.25.22.docx

---

Hello Kathy,

Revisiting the MOU discussion, after reviewing this with our Chief Legal Counsel, the Department is comfortable modifying the agreement to reflect SPD's use of its own policy. Attached are the proposed changes to that document. Please advise if this is acceptable to you.

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

Subject: FW: Updated modification request
Date: Wednesday, October 26, 2022 2:46:19 PM
Attachments: image003.png
image004.png
QT_MSP081822.1.pdf
Commonwealth_of_Massachusetts_Fusion_Center-Proposal1_copy-i2_-15675-15-Jul-2022-18-14-12.pdf
Est_2524_from_BainCor_Inc._18968.pdf
FSHSP20CFC Modification Request August 2022.docx

From: christopher.wilcox@pol.state.ma.us
To: Egnitz, Brian (POL)
Subject: Fwd: Digital Brochure
Date: Monday, June 27, 2022 8:07:29 PM
Attachments: Fusus Real-Time Crime Center In The Cloud- 2022 Brochure (1).pdf

---

LTC Chris Wilcox
Division of Homeland Security and Preparedness

Begin forwarded message:

From: Carlo Capano <ctc@fusus.com>
Date: June 27, 2022 at 7:36:51 PM EDT
To: "Wilcox, Christopher (POL)" <christopher.wilcox@pol.state.ma.us>
Subject: Digital Brochure

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,

Last is the digital brochure, if you receive this and the price list, that means the PP was the issue. I'll send it in a google drive format.

Carlo

--

Carlo Capano
Director of Sales, Northeast Region
t: +1 844-226-9226 | **m:** +1 (603) [redacted]
w: fusus.com

Fusus Events Calendar: https://www.fusus.com/about-us/fusus-events
Schedule Training: http://fusus.com/training

From: Wilcox, Christopher (POL)
To: Egnitz, Brian (POL)
Subject: Fwd: Digital Brochure
Date: Monday, June 27, 2022 8:07:31 PM
Attachments: Fusus Real-Time Crime Center In The Cloud- 2022 Brochure (1).pdf

---

LTC Chris Wilcox
Division of Homeland Security and Preparedness

Begin forwarded message:

> **From:** Carlo Capano <ctc@fusus.com>
> **Date:** June 27, 2022 at 7:36:51 PM EDT
> **To:** "Wilcox, Christopher (POL)" <christopher.wilcox@pol.state.ma.us>
> **Subject: Digital Brochure**
>
> 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,
>
> Last is the digital brochure, if you receive this and the price list, that means the PP was the issue. I'll send it in a google drive format.
>
> Carlo
>
> --
>
> **Carlo Capano**
> Director of Sales, Northeast Region
> **t:** +1 844-226-9226 | **m:** +1 (603) [redacted]
> **w:** fusus.com
>
> **Fusus Events Calendar:** https://www.fusus.com/about-us/fusus-events
> **Schedule Training:** http://fusus.com/training

From:	erik.telford@pol.state.ma.us
To:	Bellao, Shaun (POL); Trout, Jason (POL); Owerka, Jenna (POL); Micciche, John (POL); gmercurio; Reynolds, Michael J (POL); Ryan Cramer; Healy, Sean (POL)
Subject:	Fwd: Division Commander"s Orders
Date:	Wednesday, May 18, 2022 3:11:02 PM
Attachments:	DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf DC Order 2022-DHS-003 Unit Commander CCU.pdf

Erik V. Telford #2934
Detective Lieutenant
Massachusetts State Police
Division of Homeland Security and Preparedness
C.I.N.R.E.T. South
Office: 508-923-4102
Cell: 781-[redacted]

Begin forwarded message:

From: "Warren, Rosemary (POL)" <Rosemary.Warren@pol.state.ma.us>
Date: May 18, 2022 at 3:02:28 PM EDT
To: "Aumais, Matthew (POL)" <matthew.aumais@pol.state.ma.us>, "Bandini, Brian (POL)" <brian.bandini@pol.state.ma.us>, "Boyle, Christopher (DOT)" <Christopher.P.Boyle@dot.state.ma.us>, "Boyle, Christopher (POL)" <Christopher.Boyle@pol.state.ma.us>, "Brooks, Brian (POL)" <brian.brooks@pol.state.ma.us>, "Bruce, James (POL)" <James.Bruce@pol.state.ma.us>, "Conron, John (POL)" <john.conron@pol.state.ma.us>, "Crouse, David (POL)" <david.crouse@pol.state.ma.us>, "Cunningham, James (POL)" <james.cunningham@pol.state.ma.us>, "Devlin, James (CDA)" <james.devlin@mass.gov>, "Dorian, Christine (POL)" <Christine.Dorian@pol.state.ma.us>, "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state.ma.us>, "Dunn, Scott (POL)" <Scott.Dunn@pol.state.ma.us>, "Fairchild, Eric (POL)" <eric.fairchild@pol.state.ma.us>, "Gavioli, Brian (POL)" <brian.gavioli@pol.state.ma.us>, "George, Michael (POL)" <Michael.George@pol.state.ma.us>, "Goslin, John (POL)" <john.goslin@pol.state.ma.us>, "Kardoos, Albert (POL)" <albert.kardoos@pol.state.ma.us>, "Kaupp, Kevin (POL)" <kevin.kaupp@pol.state.ma.us>, "LaBarge, Robert (POL)" <Robert.LaBarge@pol.state.ma.us>, "McLaughlin, Kelly (POL)" <kelly.mclaughlin@pol.state.ma.us>, "Nason, Nicholas (POL)" <Nicholas.Nason@pol.state.ma.us>, "O'Hara, Edward (POL)" <Edward.OHara@pol.state.ma.us>, "OToole, Kevin (POL)" <kevin.otoole@pol.state.ma.us>, "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>, "Popovich, Andrew D (POL)" <Andrew.D.Popovich@pol.state.ma.us>, "Quigley, Robert (POL)" <robert.quigley@pol.state.ma.us>, "Racki, Steven M (POL)"

<Steven.M.Racki@pol.state.ma.us>, "Riley, Patricia (POL)"
<patricia.riley@pol.state.ma.us>, "Santos, John (POL)"
<john.santos@pol.state.ma.us>, "Shink, Norman (POL)"
<norman.shink@pol.state.ma.us>, "Strazzullo, John (POL)"
<john.strazzullo@pol.state.ma.us>, "Telford, Erik (POL)"
<erik.telford@pol.state.ma.us>, "Thibault, Amy (POL)"
<amy.thibault@pol.state.ma.us>, "Twomey, David (POL)"
<david.twomey@pol.state.ma.us>, "Walsh, Mark (POL)"
<Mark.Walsh@pol.state.ma.us>, "Warren, Rosemary (POL)"
<Rosemary.Warren@pol.state.ma.us>
Cc: "Cyr, Mark (POL)" <mark.cyr@pol.state.ma.us>, "Tucker, Daniel T (POL)"
<Daniel.T.Tucker@pol.state.ma.us>, "Wilcox, Christopher (POL)"
<christopher.wilcox@pol.state.ma.us>, "Murphy, Matthew G - DIS (POL)"
<matthew.g.murphy@pol.state.ma.us>, "McCarthy, Steven (POL)"
<steven.mccarthy@pol.state.ma.us>
Subject: Division Commander's Orders

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From: Telford, Erik (POL)
To: Bellao, Shaun (POL); Trout, Jason (POL); Owerka, Jenna (POL); Micciche, John (POL); gmercurio; Reynolds, Michael J (POL); Ryan Cramer; Healy, Sean (POL)
Subject: Fwd: Division Commander"s Orders
Date: Wednesday, May 18, 2022 3:11:09 PM
Attachments: DC Order 2022-DHS-002 Use of Non-Departmental ALPR Systems.pdf
DC Order 2022-DHS-003 Unit Commander CCU.pdf

Erik V. Telford #2934
Detective Lieutenant
Massachusetts State Police
Division of Homeland Security and Preparedness
C.I.N.R.E.T. South
Office: 508-923-4102
Cell: 781-[redacted]

Begin forwarded message:

From: "Warren, Rosemary (POL)" <Rosemary.Warren@pol.state.ma.us>
Date: May 18, 2022 at 3:02:28 PM EDT
To: "Aumais, Matthew (POL)" <matthew.aumais@pol.state.ma.us>, "Bandini, Brian (POL)" <brian.bandini@pol.state.ma.us>, "Boyle, Christopher (DOT)" <Christopher.P.Boyle@dot.state.ma.us>, "Boyle, Christopher (POL)" <Christopher.Boyle@pol.state.ma.us>, "Brooks, Brian (POL)" <brian.brooks@pol.state.ma.us>, "Bruce, James (POL)" <James.Bruce@pol.state.ma.us>, "Conron, John (POL)" <john.conron@pol.state.ma.us>, "Crouse, David (POL)" <david.crouse@pol.state.ma.us>, "Cunningham, James (POL)" <james.cunningham@pol.state.ma.us>, "Devlin, James (CDA)" <james.devlin@mass.gov>, "Dorian, Christine (POL)" <Christine.Dorian@pol.state.ma.us>, "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state.ma.us>, "Dunn, Scott (POL)" <Scott.Dunn@pol.state.ma.us>, "Fairchild, Eric (POL)" <eric.fairchild@pol.state.ma.us>, "Gavioli, Brian (POL)" <brian.gavioli@pol.state.ma.us>, "George, Michael (POL)" <Michael.George@pol.state.ma.us>, "Goslin, John (POL)" <john.goslin@pol.state.ma.us>, "Kardoos, Albert (POL)" <albert.kardoos@pol.state.ma.us>, "Kaupp, Kevin (POL)" <kevin.kaupp@pol.state.ma.us>, "LaBarge, Robert (POL)" <Robert.LaBarge@pol.state.ma.us>, "McLaughlin, Kelly (POL)" <kelly.mclaughlin@pol.state.ma.us>, "Nason, Nicholas (POL)" <Nicholas.Nason@pol.state.ma.us>, "O'Hara, Edward (POL)" <Edward.OHara@pol.state.ma.us>, "OToole, Kevin (POL)" <kevin.otoole@pol.state.ma.us>, "Pack, Noah (POL)" <noah.pack@pol.state.ma.us>, "Popovich, Andrew D (POL)" <Andrew.D.Popovich@pol.state.ma.us>, "Quigley, Robert (POL)" <robert.quigley@pol.state.ma.us>, "Racki, Steven M (POL)"

<Steven.M.Racki@pol.state.ma.us>, "Riley, Patricia (POL)"
<patricia.riley@pol.state.ma.us>, "Santos, John (POL)"
<john.santos@pol.state.ma.us>, "Shink, Norman (POL)"
<norman.shink@pol.state.ma.us>, "Strazzullo, John (POL)"
<john.strazzullo@pol.state.ma.us>, "Telford, Erik (POL)"
<erik.telford@pol.state.ma.us>, "Thibault, Amy (POL)"
<amy.thibault@pol.state.ma.us>, "Twomey, David (POL)"
<david.twomey@pol.state.ma.us>, "Walsh, Mark (POL)"
<Mark.Walsh@pol.state.ma.us>, "Warren, Rosemary (POL)"
<Rosemary.Warren@pol.state.ma.us>
Cc: "Cyr, Mark (POL)" <mark.cyr@pol.state.ma.us>, "Tucker, Daniel T (POL)"
<Daniel.T.Tucker@pol.state.ma.us>, "Wilcox, Christopher (POL)"
<christopher.wilcox@pol.state.ma.us>, "Murphy, Matthew G - DIS (POL)"
<matthew.g.murphy@pol.state.ma.us>, "McCarthy, Steven (POL)"
<steven.mccarthy@pol.state.ma.us>
Subject: Division Commander's Orders

Good Afternoon,

Please be advised that Division Commander's Orders 2022-DHS-002 and 2022-DHS-003 have been posted to PowerDMS. Please insure all those under your command are aware of these Orders.

Respectfully,

Rose

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

From: david.crouse@pol.state.ma.us
To: Doherty, Gregory (POL)
Subject: Fwd: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)
Date: Thursday, August 4, 2022 8:08:11 AM
Attachments: image001.png
NexusClient QRG 7.2.0 202112021640.pdf
Nexus Mobile QRG 202006171029.pdf
Copy of NEW EMS System Admin 7.2.0 202111301641.pdf

Sent from my iPhone

Begin forwarded message:

From: "Manning, David (POL)" <david.manning@pol.state.ma.us>
Date: August 3, 2022 at 9:18:42 AM EDT
To: "Deas, James (POL)" <jmdeas@pol.state.ma.us>
Cc: "Crouse, David (POL)" <david.crouse@pol.state.ma.us>, "Mcnamara, Sean (POL)" <sean.mcnamara@pol.state.ma.us>
Subject: Fw: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Trooper David M. Manning
Massachusetts State Police
Division of Homeland Security and Preparedness
Technical Services Unit

Cell: 617-[redacted]

From: Dave M <2016645@gmail.com>
Sent: Wednesday, August 3, 2022 9:15 AM
To: Manning, David (POL) <david.manning@pol.state.ma.us>
Subject: Fwd: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

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.

Sent from my iPhone

Begin forwarded message:

From: Paul Allen <paul@airshipvms.com>
Date: August 3, 2022 at 07:59:35 EDT
To: Dave Manning <2016645@gmail.com>
Cc: bob.fecteau@outlook.com, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Dave, see attached download link, was just about to hit send. If you want to download this file to the desktop we can walk through the rest of it when we do the setup. Also, if you want to download our Mobile App on your iPhone or Android pull that down in advance and we can go through the setup then. The app is called Nexus Mobile on either store / marketplace with the icon being the orange airship on a black background. Also attached to this email are the user guides for EMS and the various client applications for further review if you have questions after we get everything up and running. Look forward to the discussion later today.

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

v/r

Paul

The information contained in this transmission is confidential and/or may contain client privileged communications intended for the use of the individual or entity named above, and JDL Digital Systems (DBA Airship Industries, Inc.). If the reader of this electronic message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying is strictly prohibited.

From: Dave Manning <2016645@gmail.com>
Date: Wednesday, August 3, 2022 at 7:49 AM
To: paul@airshipvms.com <paul@airshipvms.com>
Cc: bob.fecteau@outlook.com <bob.fecteau@outlook.com>, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com <tyler@airshipvms.com>
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Thanks Paul. You mentioned previously that you would send a download link to save time. Is that something you still want to do, or shall we wait until our Zoom?

Dave

On Tue, Aug 2, 2022 at 9:34 PM <paul@airshipvms.com> wrote:

> Paul Allen is inviting you to a scheduled Zoom meeting.
>
> Join Zoom Meeting
> https://us06web.zoom.us/j/84554805559?pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
>
> Meeting ID: 845 5480 5559
> Passcode: 757394
> One tap mobile
> +13126266799,,84554805559#,,,,*757394# US (Chicago)
> +16469313860,,84554805559#,,,,*757394# US
>
> Dial by your location
> +1 312 626 6799 US (Chicago)
> +1 646 931 3860 US
> +1 929 436 2866 US (New York)
> +1 301 715 8592 US (Washington DC)
> +1 669 900 6833 US (San Jose)
> +1 253 215 8782 US (Tacoma)
> +1 346 248 7799 US (Houston)
> +1 386 347 5053 US
> +1 564 217 2000 US
> +1 669 444 9171 US
> Meeting ID: 845 5480 5559
> Passcode: 757394
> Find your local number:
> https://us06web.zoom.us/u/kMEG8yJaM
>
> **When**
>
> Wednesday Aug 3, 2022 · 12pm – 1pm (Eastern Time - New York)
>
> **Location**
>
> https://us06web.zoom.us/j/84554805559?

pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
View map

Guests

paul@airshipvms.com - organizer
2016645@gmail.com
bob.fecteau@outlook.com
Dominic Splattstoesser
tyler@airshipvms.com
View all guest info

Reply for 2016645@gmail.com

Yes | No | Maybe

More options

Invitation from Google Calendar

You are receiving this email because you are subscribed to calendar notifications. To stop receiving these emails, go to Calendar settings, select this calendar, and change "Other notifications".

Forwarding this invitation could allow any recipient to send a response to the organizer, be added to the guest list, invite others regardless of their own invitation status, or modify your RSVP. Learn more

From: Dave M
To: Manning, David (POL)
Subject: Fwd: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)
Date: Wednesday, August 3, 2022 9:17:53 AM
Attachments: image001.png
NexusClient QRG 7.2.0 202112021640.pdf
Nexus Mobile QRG 202006171029.pdf
Copy of NEW EMS System Admin 7.2.0 202111301641.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.

Sent from my iPhone

Begin forwarded message:

From: Paul Allen <paul@airshipvms.com>
Date: August 3, 2022 at 07:59:35 EDT
To: Dave Manning <2016645@gmail.com>
Cc: bob.fecteau@outlook.com, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Dave, see attached download link, was just about to hit send. If you want to download this file to the desktop we can walk through the rest of it when we do the setup. Also, if you want to download our Mobile App on your iPhone or Android pull that down in advance and we can go through the setup then. The app is called Nexus Mobile on either store / marketplace with the icon being the orange airship on a black background. Also attached to this email are the user guides for EMS and the various client applications for further review if you have questions after we get everything up and running. Look forward to the discussion later today.

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

Paul

Paul Allen
President
AIRSHIP Industries, Inc.,
12226 134th CT NE
Redmond, WA 98052
704.798.7973

The information contained in this transmission is confidential and/or may contain client privileged communications intended for the use of the individual or entity named above, and JDL Digital Systems (DBA Airship Industries, Inc.). If the reader of this electronic message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying is strictly prohibited.

From: Dave Manning <2016645@gmail.com>
Date: Wednesday, August 3, 2022 at 7:49 AM
To: paul@airshipvms.com <paul@airshipvms.com>
Cc: bob.fecteau@outlook.com <bob.fecteau@outlook.com>, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com <tyler@airshipvms.com>
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Thanks Paul. You mentioned previously that you would send a download link to save time. Is that something you still want to do, or shall we wait until our Zoom?

Dave

On Tue, Aug 2, 2022 at 9:34 PM <paul@airshipvms.com> wrote:

> Paul Allen is inviting you to a scheduled Zoom meeting.
>
> Join Zoom Meeting
> https://us06web.zoom.us/j/84554805559?pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
>
> Meeting ID: 845 5480 5559
> Passcode: 757394
> One tap mobile

+13126266799,,84554805559#,,,,*757394# US (Chicago)
+16469313860,,84554805559#,,,,*757394# US

Dial by your location
+1 312 626 6799 US (Chicago)
+1 646 931 3860 US
+1 929 436 2866 US (New York)
+1 301 715 8592 US (Washington DC)
+1 669 900 6833 US (San Jose)
+1 253 215 8782 US (Tacoma)
+1 346 248 7799 US (Houston)
+1 386 347 5053 US
+1 564 217 2000 US
+1 669 444 9171 US
Meeting ID: 845 5480 5559
Passcode: 757394
Find your local number: https://us06web.zoom.us/u/kMEG8yJaM

When

Wednesday Aug 3, 2022 · 12pm – 1pm (Eastern Time - New York)

Location

https://us06web.zoom.us/j/84554805559?pwd=SnhaK3RDMjRsZHlrMUh0VytsK3RVQT09
View map

Guests

paul@airshipvms.com - organizer
2016645@gmail.com
bob.fecteau@outlook.com
Dominic Splattstoesser
tyler@airshipvms.com
View all guest info

Reply for 2016645@gmail.com

Yes | No | Maybe

More options

Invitation from Google Calendar

You are receiving this email because you are subscribed to calendar notifications. To stop receiving these emails, go to Calendar settings, select this calendar, and change "Other notifications".

Forwarding this invitation could allow any recipient to send a response to the organizer, be added to the guest list, invite others regardless of their own invitation status, or modify your RSVP. Learn more

From:	Crouse, David (POL)
To:	Doherty, Gregory (POL)
Subject:	Fwd: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)
Date:	Thursday, August 4, 2022 8:08:15 AM
Attachments:	image001.png NexusClient QRG 7.2.0 202112021640.pdf Nexus Mobile QRG 202006171029.pdf Copy of NEW EMS System Admin 7.2.0 202111301641.pdf

Sent from my iPhone

Begin forwarded message:

From: "Manning, David (POL)" <david.manning@pol.state.ma.us>
Date: August 3, 2022 at 9:18:42 AM EDT
To: "Deas, James (POL)" <jmdeas@pol.state.ma.us>
Cc: "Crouse, David (POL)" <david.crouse@pol.state.ma.us>, "Mcnamara, Sean (POL)" <sean.mcnamara@pol.state.ma.us>
Subject: Fw: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Trooper David M. Manning
Massachusetts State Police
Division of Homeland Security and Preparedness
Technical Services Unit

Cell: 617-[redacted]

From: Dave M <2016645@gmail.com>
Sent: Wednesday, August 3, 2022 9:15 AM
To: Manning, David (POL) <david.manning@pol.state.ma.us>
Subject: Fwd: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

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.

Sent from my iPhone

Begin forwarded message:

From: Paul Allen <paul@airshipvms.com>
Date: August 3, 2022 at 07:59:35 EDT
To: Dave Manning <2016645@gmail.com>
Cc: bob.fecteau@outlook.com, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Dave, see attached download link, was just about to hit send. If you want to download this file to the desktop we can walk through the rest of it when we do the setup. Also, if you want to download our Mobile App on your iPhone or Android pull that down in advance and we can go through the setup then. The app is called Nexus Mobile on either store / marketplace with the icon being the orange airship on a black background. Also attached to this email are the user guides for EMS and the various client applications for further review if you have questions after we get everything up and running. Look forward to the discussion later today.

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

v/r

Paul

The information contained in this transmission is confidential and/or may contain client privileged communications intended for the use of the individual or entity named above, and JDL Digital Systems (DBA Airship Industries, Inc.). If the reader of this electronic message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying is strictly prohibited.

From: Dave Manning <2016645@gmail.com>
Date: Wednesday, August 3, 2022 at 7:49 AM
To: paul@airshipvms.com <paul@airshipvms.com>
Cc: bob.fecteau@outlook.com <bob.fecteau@outlook.com>, Dominic Splattstoesser <nic@airshipvms.com>, tyler@airshipvms.com <tyler@airshipvms.com>
Subject: Re: Invitation: Mass State Police Install @ Wed Aug 3, 2022 12pm - 1pm (EDT) (2016645@gmail.com)

Thanks Paul. You mentioned previously that you would send a download link to save time. Is that something you still want to do, or shall we wait until our Zoom?

Dave

On Tue, Aug 2, 2022 at 9:34 PM <paul@airshipvms.com> wrote:

> Paul Allen is inviting you to a scheduled Zoom meeting.
>
> Join Zoom Meeting
> https://us06web.zoom.us/j/84554805559?pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
>
> Meeting ID: 845 5480 5559
> Passcode: 757394
> One tap mobile
> +13126266799,,84554805559#,,,,*757394# US (Chicago)
> +16469313860,,84554805559#,,,,*757394# US
>
> Dial by your location
> +1 312 626 6799 US (Chicago)
> +1 646 931 3860 US
> +1 929 436 2866 US (New York)
> +1 301 715 8592 US (Washington DC)
> +1 669 900 6833 US (San Jose)
> +1 253 215 8782 US (Tacoma)
> +1 346 248 7799 US (Houston)
> +1 386 347 5053 US
> +1 564 217 2000 US
> +1 669 444 9171 US
> Meeting ID: 845 5480 5559
> Passcode: 757394
> Find your local number:
> https://us06web.zoom.us/u/kMEG8yJaM
>
> **When**
>
> Wednesday Aug 3, 2022 · 12pm – 1pm (Eastern Time - New York)
>
> **Location**
>
> https://us06web.zoom.us/j/84554805559?

pwd=SnhaK3RDMjRsZHlrMUhOVytsK3RVQT09
View map

Guests

paul@airshipvms.com - organizer
2016645@gmail.com
bob.fecteau@outlook.com
Dominic Splattstoesser
tyler@airshipvms.com
View all guest info

Reply for 2016645@gmail.com

Yes | No | Maybe

More options

Invitation from Google Calendar

You are receiving this email because you are subscribed to calendar notifications. To stop receiving these emails, go to Calendar settings, select this calendar, and change "Other notifications".

Forwarding this invitation could allow any recipient to send a response to the organizer, be added to the guest list, invite others regardless of their own invitation status, or modify your RSVP. Learn more

From: David.M.Dicicco@pol.state.ma.us
To: Connor, Greg (NFK); Monahan, Meagen (NFK)
Subject: Fwd: LPRs
Date: Wednesday, December 7, 2022 9:01:31 AM
Attachments: Commonwealth v McCarthy.doc

Not sure how this factors in to our case where we used flock cam.

Dave.

Sent from my iPhone

Begin forwarded message:

> **From:** "Beatty, Lisa (NFK)" <lisa.beatty@mass.gov>
> **Date:** December 7, 2022 at 8:54:44 AM EST
> **To:** "Kotkowski, Jeffrey (POL)" <jeffrey.kotkowski@pol.state.ma.us>, "Paris, Charles" <cparis@braintreema.gov>
> **Cc:** "Dicicco, David M (POL)" <David.M.Dicicco@pol.state.ma.us>
> **Subject: FW: LPRs**
>
> FYI
>
> ---
>
> **From:** Alford, Pamela (NFK) <pamela.alford@mass.gov>
> **Sent:** Wednesday, December 7, 2022 6:20 AM
> **To:** Beatty, Lisa (NFK) <lisa.beatty@mass.gov>
> **Subject:** LPRs
>
> Lisa:
>
> As to LPRs, there may be several obstacles as to admissibility.
>
> First, it is unclear whether the amount of data would implicate the defendants' reasonable expectation of privacy to the extent that the records would be amenable to a MTS for lack of search warrant. The case on point is Commonwealth v. McCarthy, 484 Mass. 493 (2020). The SJC found that four cameras on a bridge was not enough. Factors in our favor is that the cameras appear to be on highways and spread out, so there is not a tracking of the intimate features of life under the mosaic theory. On the other hand, there is more separate places of tracking here than in McCarthy.
>
> Second, according to media reports, MSP discontinued this system as of Dec. 2020 (I believe we got the memo). Unclear what they are doing now. There was a reliability issue with the specific cameras as to the date and time. In McCarthy, the parties ended

up redoing the MTS, without the LPR info, which was allowed and the case np'd. I did not see any MA case on westlaw where LPRs had been admitted at trial.

Third, as to business records, subpoenas would likely have to go to the organizations that keep those records. Is it correct that the Fusion Center is a subscriber, but itself would not keep LPR records as a part of its business? We likely would need the originator (similar to a phone company). For the NYC, we would need someone from their PD. They keep records for five years unless marked as part of an investigation. See NYPD 2021 policy governing such use - license-plate-readers-lpr-nypd-impact-and-use-policy_4.9.21_final.pdf (nyc.gov)

Happy to discuss.
Pamela

From: Dicicco, David M (POL)
To: Connor, Greg (NFK); Monahan, Meagen (NFK)
Subject: Fwd: LPRs
Date: Wednesday, December 7, 2022 9:01:32 AM
Attachments: Commonwealth v McCarthy.doc

Not sure how this factors in to our case where we used flock cam.

Dave.

Sent from my iPhone

Begin forwarded message:

> **From:** "Beatty, Lisa (NFK)" <lisa.beatty@mass.gov>
> **Date:** December 7, 2022 at 8:54:44 AM EST
> **To:** "Kotkowski, Jeffrey (POL)" <jeffrey.kotkowski@pol.state.ma.us>, "Paris, Charles" <cparis@braintreema.gov>
> **Cc:** "Dicicco, David M (POL)" <David.M.Dicicco@pol.state.ma.us>
> **Subject: FW: LPRs**
>
> FYI
>
> ---
>
> **From:** Alford, Pamela (NFK) <pamela.alford@mass.gov>
> **Sent:** Wednesday, December 7, 2022 6:20 AM
> **To:** Beatty, Lisa (NFK) <lisa.beatty@mass.gov>
> **Subject:** LPRs
>
> Lisa:
>
> As to LPRs, there may be several obstacles as to admissibility.
>
> First, it is unclear whether the amount of data would implicate the defendants' reasonable expectation of privacy to the extent that the records would be amenable to a MTS for lack of search warrant. The case on point is Commonwealth v. McCarthy, 484 Mass. 493 (2020). The SJC found that four cameras on a bridge was not enough. Factors in our favor is that the cameras appear to be on highways and spread out, so there is not a tracking of the intimate features of life under the mosaic theory. On the other hand, there is more separate places of tracking here than in McCarthy.
>
> Second, according to media reports, MSP discontinued this system as of Dec. 2020 (I believe we got the memo). Unclear what they are doing now. There was a reliability issue with the specific cameras as to the date and time. In McCarthy, the parties ended

up redoing the MTS, without the LPR info, which was allowed and the case np'd. I did not see any MA case on westlaw where LPRs had been admitted at trial.

Third, as to business records, subpoenas would likely have to go to the organizations that keep those records. Is it correct that the Fusion Center is a subscriber, but itself would not keep LPR records as a part of its business? We likely would need the originator (similar to a phone company). For the NYC, we would need someone from their PD. They keep records for five years unless marked as part of an investigation. See NYPD 2021 policy governing such use - license-plate-readers-lpr-nypd-impact-and-use-policy_4.9.21_final.pdf (nyc.gov)

Happy to discuss.
Pamela

From: Clark, James (POL)
To: jamesrclark@gmail com
Subject: Fwd: massDOT question
Date: Thursday, March 10, 2022 8:44:03 AM
Attachments: SCF_MSP_Ba nCor_executed.pdf
MBPO 24335.PDF
2020_MAR_Telecomm_RFR_F nal-Rev sed-July docx
image001.png
image002.png
im_ge003.png

Sent from my iPhone
Please excuse any typos/brevity

From: Biagi Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Sent: Wednesday January 26 2022 1 29 03 PM
To: Clark James (POL) <James.Clark@pol.state.ma.us>; Doherty Nancy (POL) <Nancy.Doherty@pol.state.ma.us>; Gray Kellie (POL) <Kellie.Gray@pol.state.ma.us>; LeBlanc Nicole (POL) <Nicole.LeBlanc2@pol.state.ma.us>; Meagher Ann (POL) <Ann.Meagher@pol.state.ma.us>; Pearson Gustav (POL) <Gustav.Pearson@pol.state.ma.us>; Yanoff Benjamin (POL) <Benjamin.Yanoff@pol.state.ma.us>
Subject: FW massDOT question

FYI

Pamela Biagi
Director of Fiscal Services
Massachusetts State Police
470 Worcester Rd
Framingham, MA 01702
508-820-2126
Pamela Biagi@pol state ma us

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Wednesday January 26 2022 12 15 PM
To: Biagi Pamela (POL) <Pamela.Biagi@pol.state.ma.us>
Cc: Silva Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rossi Gina (POL) <Gina.Rossi@pol.state.ma.us>
Subject: FW massDOT question

Hi Pam

FYI. This is a "piggyback" contract through MassDOT. Division of Homeland Security was hoping to use BainCor to purchase ALPR solar trailers.

MassDOT added us to their MA. Dianne included the MA number below.

As for the MBPO MassDOT does not create MBPO s in COMMBUYS currently. Only bid solicitations. Therefore Dianne did a direct PO to the vendor in this case referencing the MassDOT contract. Number below/attached.

Thank you
Brian

From: Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 57 AM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Rossi Gina (POL) <Gina Rossi@pol state ma us>
Subject: RE massDOT question

Hi Brian
I wasn t sure who the purchasing info would go to.

MMARS MA DOT INFT0000K03C00111753
COMMBUYS MBPO PO-22-1084-POLGH-GHQ-24335

Expires 6/30/2025

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Wednesday January 26 2022 11 06 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>; Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Thank you everyone for the assistance. It is much appreciated.

Sincerely

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian J Kearnan@pol state ma us

From: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Sent: Wednesday January 26 2022 10 59 AM
To: Lee Daniel (DOT) <Daniel Lee@dot state ma us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE massDOT question

Hi Dan

Department of State Police (POL) has bee added to MA INTF0000K03C00111753 version 10 and is now final.

Mary Mariani
Accountant III
MassDOT
10 Park Plaza, Ste 5450
Boston, MA 02116
mary.mariani@state.ma.us
(P) 857-368-9068
(F) 857-368-0637

From: Lee Daniel (DOT) <Daniel Lee@dot state ma us>
Sent: Wednesday January 26 2022 10 25 AM
To: Mariani Mary (DOT) <Mary.Mariani@dot.state.ma.us>
Cc: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>; Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Mary – can you please add POL as an authorized Department for MA DOT INTF0000K03C00111753 and let everyone on this e-mail know when it has been put to Final in MMARS.

Thank You!

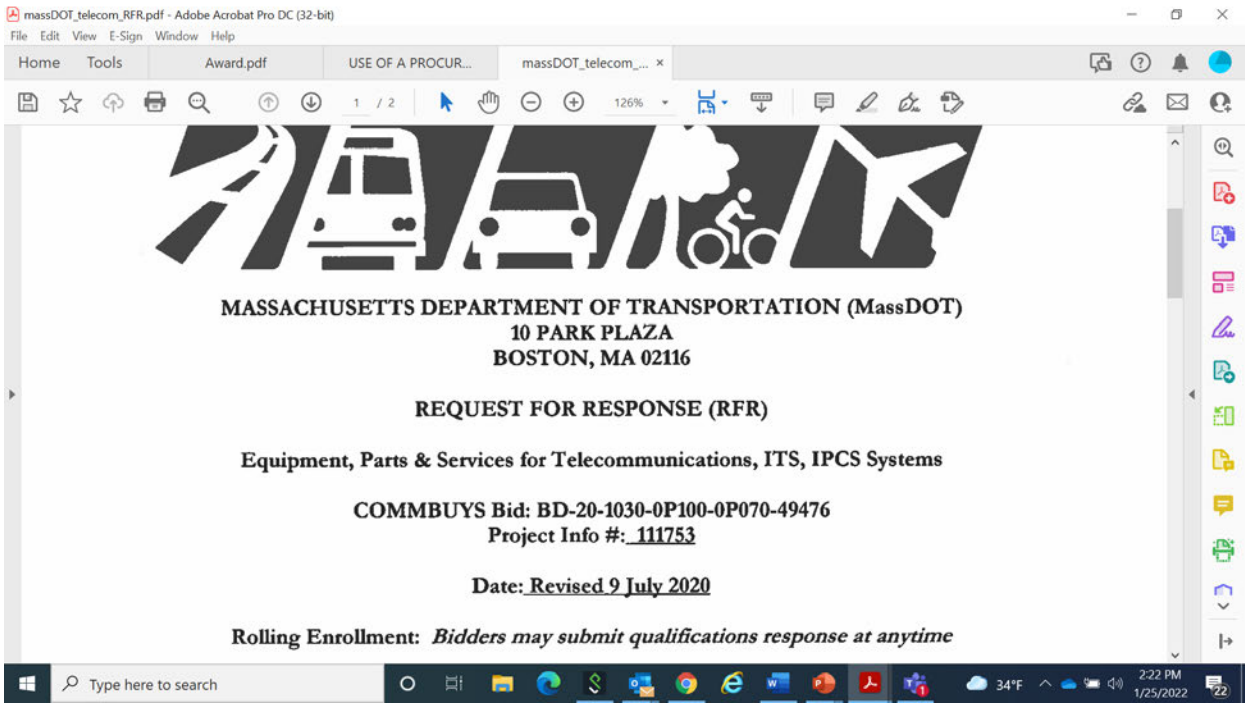
Daniel Lee
Deputy Director of Accounting
10 Park Plaza – Suite 5510
Boston, MA 02116
Phone: (857)-368-9074
Work Cell: (617) [redacted]

From: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday January 25 2022 2 27 PM
To: Lee Daniel (DOT) <Daniel.Lee@dot.state.ma.us>
Cc: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>; Miller Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FW massDOT question

Hi Dan

I have granted POL permission to access the contract you see below. Can you please confirm if there is a MA for this and if there is can you please add POL as an authorized user and share the MA # with our friends from POL cc d here?

Thank you Dan.


massDOT_telecom_RFR.pdf - Adobe Acrobat Pro DC (32-bit)

MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MassDOT)
10 PARK PLAZA
BOSTON, MA 02116

REQUEST FOR RESPONSE (RFR)

Equipment, Parts & Services for Telecommunications, ITS, IPCS Systems

COMMBUYS Bid: BD-20-1030-0P100-0P070-49476
Project Info #: 111753

Date: Revised 9 July 2020

Rolling Enrollment: *Bidders may submit qualifications response at anytime*

From: Bianchi John D. (DOT)
Sent: Tuesday January 18 2022 1 48 PM
To: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE massDOT question

Hi Brian

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it s open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet which will include the executed SCF. Once I receive it I will pass it along to you.

From: Kearnan Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday January 18 2022 1 38 PM
To: Bianchi John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn t heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Pack, Noah (POL)
To: Nelj@seekonkpd.com
Cc: sgt.hedrick@seekonkpd.com
Subject: Fwd: Mobile LPR Update
Date: Saturday, May 28, 2022 3:50:41 PM
Attachments: TRF-11 Nov21.pdf
ALPR TENANT MOU.docx

Hi Jim,

I'm reaching out regarding your mobile LPR. We would like to get you switched over to the new system, as the old server will be shut down shortly.

I'd like to determine if your system has been updated by Kory Koster or another BCM tech or if that still needs to be done.

Additionally, there is an MOU required as part of the new system. I've the attached the MOU and our MSP policy for your review. When that is returned to us we can get you switched over. Please let me know if you have any questions.

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: Hedrick, Thomas <sgt.hedrick@seekonkpd.com>
Sent: Saturday, May 28, 2022 15:38
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Mobile LPR Update

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.

Sorry thought I did Nelj@seekonkpd.com

Thomas Hedrick
Sergeant
Seekonk police
508-336-8123
Ext 51116

Cellular inter web device

CONFIDENTIALITY AND INADVERTENT DISCLOSURE NOTICE:
This e-mail transmission may contain confidential information belonging to the sender which is legally privileged and which is only intended for the use of the intended recipient. If you have received this e-mail in error, such transmission is an inadvertent disclosure, and any copying, disclosure, distribution or dissemination of this information or the taking of any action based on the contents of this communication is strictly prohibited. Please notify me immediately of any inadvertent disclosure by e-mail, delete the original transmission and destroy any printouts you may have made.

On May 28, 2022, at 15:35, Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

Sgt Hedrick,

Thanks for your response. There is an MOU that is now required for the new LPR system. I'm happy to send that to Officer Nelson if you could please send me his contact information.

Respectfully,

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: Hedrick, Thomas <sgt.hedrick@seekonkpd.com>
Sent: Saturday, May 28, 2022 10:42
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Mobile LPR Update

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,

Reach out to Officer Jim Nelson. The vehicle is assigned to him. Keep me in the loop please.

Thank you,

Thomas Hedrick
Sergeant / IT
Seekonk police

508-336-8123
Ext 51116

Cellular inter web device

CONFIDENTIALITY AND INADVERTENT DISCLOSURE NOTICE:
This e-mail transmission may contain confidential information belonging to the sender which is legally privileged and which is only intended for the use of the intended recipient. If you have received this e-mail in error, such transmission is an inadvertent disclosure, and any copying, disclosure, distribution or dissemination of this information or the taking of any action based on the contents of this communication is strictly prohibited. Please notify me immediately of any inadvertent disclosure by e-mail, delete the original transmission and destroy any printouts you may have made.

On May 28, 2022, at 09:59, Pack, Noah (POL) <noah.pack@state.ma.us> wrote:

Good morning sir,

I received your contact information from BCM controls, and I'm reaching out regarding your mobile LPR unit. If it is still in service or you are trying to get it back in service, we'd like to help you migrate them into the new Boss4 system, as the old server will be shut down shortly.

If you have a moment to discuss this process, feel free to give me a call or let me know a good time to reach out to the appropriate person.

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
Cell: 508-[redacted]

From: Fecteau, Robert
To: Pack, Noah (POL)
Subject: Genetec LPR
Date: Wednesday, February 2, 2022 2:45:52 PM
Attachments: image001.png
image002.png
image003.png
image004.png
AutoVu-SharpV-Datasheet.pdf
ProductSpecs_EN_AutoVu-SharpZ3_WEB.pdf
EN_ALPR for Public Safety (1).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 Sir:
Attached, please find the most current datasheets on Genetec's LPR hardware. The SharpV is the camera that is used for fixed applications, while the SharpZ3 is used for mobile.

I'm working to find some relevant/representative information on the user interfaces (patroller and security desk), as the information on the partner portal is very bland/salesy.

I found an 'ALPR for Law Enforcement' product bulletin that wasn't too bad (a little dated…..still references the previous version mobile camera), and have attached that, as well.

I'll send along 'software info' as I find it.

FYI,
Bob

COMFORT SYSTEMS USA
BCM Controls Corporation

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

From: Fecteau, Robert
To: Crouse, David (POL)
Subject: Genetec NDA
Date: Thursday, February 10, 2022 2:35:24 PM
Attachments: image001.png
image002.png
image003.png
image004.png
Massachusetts State Police_NDA_Feb 2022.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 Dave,
As a follow up to our discussion of the other day, could you please sign and return the attached Genetec NDA (for the demo LPR product)?

I'm told the demo units are ready to ship.

Thanks,
Bob

COMFORT SYSTEMS USA
BCM Controls Corporation

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

From: Sullivan, Margaret (POL)
To: Cormier, Donald (POL)
Subject: Global Justice Public Safety Agreement
Date: Thursday, May 5, 2022 12:19:00 PM
Attachments: Global Justice Public Safety Agreement FINAL 9-28-2020.docx

---

Hello Capt. Cormier – Attached is the most recent Global Sharing Agreement. Once it is signed by MSP, it needs to be returned to DCJIS for the Commissioner's signature. Let me know if you have questions. -peg

Margaret Sullivan | Executive Office of Public Safety and Security
Director | Application Development and Support Services
Office of Technology and Information Services
470 Worcester Road
Framingham, MA 01702
p. 508-820-2227 | f. 508-820-2359

From: Amaral, Andrew A (POL)
To: Lorenco, Nicholas (POL); Morris, James (POL)
Subject: homework
Date: Friday, April 1, 2022 6:02:22 PM
Attachments: Q1-2022-Guardian-FINAL.pdf

Sgt,

please read and let me know your thoughts...

Trooper Andrew A. Amaral ID #3737
Mass State Police-CVES
906 Elm Street
Concord, MA 01742
Office (978) 369-1004
Fax (978) 369-5353

From: John Tedona
To: Pack, Noah (POL)
Subject: Local Agency BOSS Access
Date: Tuesday, February 1, 2022 2:22:05 PM
Attachments: image001.png
image002.png
image003.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.

Hi Noah,

I've received a few calls from local agencies (most recently Attleboro PD) wishing to connect their mobile systems to BOSS4. At present are they only allowed to connect to BOSS3 and download hotlists only with no reads being pushed to BOSS3, or assuming the local agencies have the latest mobile software (version 214.1.5 that has the time/date image watermark) I'm curious if the you are allowing the local agencies to connect to BOSS4 to push read data and download hotlists.

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

From: Salvatore, Justin (POL)
To: Bennett, Marcy (POL); Grunewald, Brady (POL); Franquiz, Andrew (POL)
Cc: Palmer, David (POL)
Subject: LPR Decision - Commonwealth vs. McCarthy
Date: Wednesday, May 4, 2022 8:42:31 PM
Attachments: Commonwealth vs. Jason J. McCarthy.pdf

Good Evening,

Attached is the MA Supreme Judicial Court decision I mentioned earlier involving the use of LPRs. Below is a link to the Harvard Law Review's analysis of the case, which I found helpful.

https://harvardlawreview.org/2021/06/commonwealth-v-mccarthy/

Respectfully,
Justin

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

From: Pack, Noah (POL)
To: mbryant@yarmouth.ma.us
Subject: LPR Tenant MOU
Date: Thursday, March 24, 2022 9:29:00 AM
Attachments: TRF-11 Nov21.pdf
ALPR TENANT MOU.docx

Lieutenant Bryant,

Please see the attached tenant MOU and MSP policy. Thank you for your understanding and assistance.

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: Pack, Noah (POL)
To: Connolly, Kevin
Subject: LPR Tenant MOU
Date: Wednesday, March 23, 2022 9:50:00 AM
Attachments: ALPR TENANT MOU.docx

Hi Kevin,

Attached is the MOU that we discussed.

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: Pack, Noah (POL)
To: Schwarz, William J
Subject: LPR Tenant MOU
Date: Friday, April 1, 2022 2:56:01 PM
Attachments: TRF-11 Nov21.pdf
ALPR TENANT MOU.docx

Hi Bill,

Please see the attached LPR Tenant MOU from our legal section and a copy of our current policy. I look forward to seeing you next week and getting you guys on board as soon as possible. Have a great weekend.

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: Pack, Noah (POL)
To: Handfield, Kenneth (POL); Barstow, Matthew (POL)
Cc: Cyr, Mark (POL); Tucker, Daniel T (POL)
Subject: LPR Training for Dispatchers
Date: Thursday, September 29, 2022 12:13:14 PM
Attachments: Guidelines for DSU LPR 9-22.pdf

Good afternoon Ken and Matt,

Training Dates & Use Guidelines

The LPR guidelines have been approved; a copy is attached for your review and has also been sent by DHS Command to DAS Command. Please feel free to reach out with any questions.

Training will include how the system can be accessed, lawful and authorized uses, and guidelines regarding LPR data and searches for DSU. The training will be conducted via Teams and should take approximately 1 to 1.5 hours. This training is intended for dispatch supervisors, although any interested dispatchers may attend. The guidelines handout will be provided during the training. The dates are as follows:

October 6: 08:00
October 11: 13:00
October 11: 21:00

System Access

The primary resource for use of the LPR system will continue to be the Commonwealth Watch Center (CWC) at GHQ, which is staffed 24/7. DHS is able to provide some system accounts to dispatch supervisors to access the system consistent with policy and the attached guidelines. We are unable to provide unlimited accounts, so we will prioritize accounts for regional dispatch centers with LPRs in their AOR, including: AHQ, B-7, BHQ, CHQ, DHQ, FHQ, and HHQ. There are no MSP LPRs in the C-8 area, and CWC will handle requests for their co-located partners at GHQ.

Please disseminate the following link for members to select a training date:
https://forms.office.com/Pages/ResponsePage.aspx?id=Fh2GPrdIDkqYBowE2Bt7KliTEFUE4v1Fo2Vn2vowRlJUQTg4TE1GV05aRjQ4UVVZRjROTDQzRlI3Qi4u

Any user who will be receiving an account must attend one of the trainings. Once they have selected a training date, we will create their accounts and send further access instructions. Any dispatchers interesting in learning about LPR but who will not be getting an account may also attend but do not need to sign up in advance.

I look forward to working with your team soon.

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: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>
Sent: Thursday, August 18, 2022 9:26 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Barstow, Matthew (POL) <matthew.barstow@pol.state.ma.us>
Subject: RE: LPR Training for Dispatchers

Hi Noah,

Matt and I have discussed this, and we are good to go when you are. Just identify some dates and times for the training and I'll make sure our people attend. In keeping with our earlier conversation, three sessions scattered throughout a day would make it easier for mid and eve shift to attend. Perhaps 07:30/08;00, 13:00/13:30, and 21:00/21:30?

Here is a proposed list of user accounts. This includes all center and shift supervisors at our 9 communications centers. Some of our dispatch centers have a minimum staffing of one (1), so there will be occasions when a supervisor is unavailable. Perhaps we could include all dispatchers at GHQ? This would allow us to always have someone able to access the LPR when a supervisor is unavailable.

I'm in the office all day today and on cell tomorrow if you want to discuss.

Thanks!
~K

		G.L. c. 4 §7 cl. 26(n) (security); G.L. ch. 4	
Cheverie, Peter J.	SPDIII	[redacted]	peter.cheverie@mass.gov
Dunphy, Angela L.	SPDII		angela.dunphy@mass.gov
Steinel, Lori D.	SPDII		lori.steinel@mass.gov
Garrity, Charles E., III	SPDIII		charles.garrity@mass.gov
de los Santos, Amanda	SPDII		amanda.flechsig@mass.gov
Patterson, Douglas T.	SPDII		douglas.patterson@mass.gov
Quinn, Heather L.	SPDII		heather.quinn@mass.gov
Dunphy, Thomas J.	SPDIII		thomas.dunphy@mass.gov
Ouimette, Kendra N.	SPDII		kendra.ouimette@mass.gov
Pariseau, Wendy J.	SPDII		wendy.pariseau@mass.gov
Reardon, Erin B.	SPDII		erin.reardon@mass.gov
Santiago, Ervin	SPDII		ervin.santiago@mass.gov

Tatro, Jeffrey R.	SPDII	[redacted]	jeffrey.tatro@mass.gov
Tryon, Donald	SPDII		donald.tryon@mass.gov
Snow, Corrine A.	SPDIII		corrine.snow@mass.gov
Doxey, Dana	SPDII		dana.doxey@mass.gov
Hanbury, Jason	SPDII		jason.hanbury@mass.gov
Snow, Wendy J.	SPDII		wendy.snow@mass.gov
Keville, Robert R.	SPDIII		robert.keville@mass.gov
Girouard, Melissa L.	SPDII		melissa.l.girouard@mass.gov
Walker, Kimberly J.	SPDII		kimberly.walker@mass.gov
Dunbar, Cameron H.	QCIII		cameron.dunbar@mass.gov
Barstow, Matthew C.	DOT		matthew.barstow@mass.gov
Handfield, Kenneth E., Jr.	DODS		kenneth.handfield@mass.gov
Demers, Joanne E.	SPDIII		joanne.demers@mass.gov
McCann, Joseph M.	SPDII		joseph.mccann@mass.gov
Ronayne, Adam J.	SPDII		adam.ronayne@mass.gov
Gleason, Kristin M.	SPDIII		kristin.gleason@mass.gov
Fredholm, Noreen S.	SPDII		shana.fredholm@mass.gov
Levesque, Joseph	SPDII		joseph.levesque@mass.gov
Ross, Jonathan C.	SPDIII		jonathan.ross@mass.gov
Kilmain, Kevin M.	SPDII		kevin.kilmain@mass.gov
Justinski, Keith A.	SPDII		keith.justinski@mass.gov
Slater, Michael K.	SPDIII		michael.slater@mass.gov
Teevens, Richard E., Jr.	SPDII		richard.teevens@mass.gov
Tilden, Charles S., Jr.	SPDII		charles.tilden@mass.gov

Costanzo, Robert	SPDI		robert.costanzo@mass.gov
Costello, Paul A.	SPDI		paul.costello@mass.gov
McGrail, Robert	SPDI		robert.mcgrail@mass.gov
Puckett, Daniel L.	SPDI		daniel.puckett@mass.gov
Simpson, Lara C.	SPDI		lara.simpson@mass.gov

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police
Communications Section, Dispatch Services Unit
50 Maple Street, Rm. 222
Milford, MA 01757

Office: 508.820.2347
Cell & Text: [redacted]

Fax: 774.462.3768 (Milford)

Email: Kenneth.Handfield@Mass.gov

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, August 18, 2022 7:47 AM
To: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>; Barstow, Matthew (POL) <matthew.barstow@pol.state.ma.us>
Subject: LPR Training for Dispatchers

Hi Matt and Ken,

DHS would like to bring the Dispatch Services Unit up to speed on the Department's license plate reader program. We are preparing a training and a handout that will include discussion of how the system can be accessed, lawful and authorized uses, and guidelines regarding LPR data and searches. The training will most likely be conducted via Teams and should take approximately 1 to 1.5 hours.

Within the next couple weeks, I would like to go over the training and guidelines with one or both of you to ensure we are on the same page and in compliance with any policy/procedure or union issues regarding your staff. In addition to the training, I have been authorized to set up system accounts for authorized dispatch supervisors. During our discussion about the training/guidelines, I'd also like to discuss the best way to set up and issue these accounts to your staff.

If this sounds acceptable, I look forward to discussing further in the near future.

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: O"Toole, Mark
To: Pack, Noah (POL)
Subject: Lynn PD ALPR Policy
Date: Tuesday, January 25, 2022 4:45:58 PM
Attachments: Lynn PD - ALPR Updated Policy - 12-2-21.docx
LPD Flock ALPR Activity.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.

Noah,

Attached is the Lynn PD ALPR Policy as amended on 12/2/21. I also attached the log I am keeping regarding our activity – success stories using the platform. I also confirmed that I gave Gary Ferguson access to our Flock database on 12/11/21. Please let me know if there is any additional information you need.

Capt. Mark O'Toole
Lynn PD Detectives
(781)[redacted] (Cell)

From: Kelly, Christopher (AGO)
To: Driscoll, Francis (POL)
Date: Monday, August 1, 2022 12:55:03 PM
Attachments: MDEG Second Version 062021.pdf
Digital Evidence Guide 062021.docx

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

From: Pack, Noah (POL)
To: Wilcox, Christopher (POL)
Date: Thursday, February 10, 2022 7:48:00 PM
Attachments: presentation draft.zip

Sir, draft attached for your review.

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: Pack, Noah (POL)
To: Egnitz, Brian (POL)
Date: Thursday, February 10, 2022 6:52:43 PM
Attachments: presentation draft.zip

From: Pack, Noah (POL)
To: Egnitz, Brian (POL)
Date: Thursday, February 10, 2022 1:11:18 PM
Attachments: presentation draft.zip

Date: Friday, January 21, 2022 1:50:41 PM
Attachments: MSP IT Project List as Jan 20 22.xlsx

Margaret Sullivan | Executive Office of Public Safety and Security
Director | Application Development and Support Services
Office of Technology and Information Services
470 Worcester Road
Framingham, MA 01702
p. 508-820-2227 | f. 508-820-2359

From: Pack, Noah (POL)
To: Egnitz, Brian (POL)
Date: Thursday, January 20, 2022 11:11:00 AM
Attachments: MOU DRAFT.docx

Can you take a look at this and let me know what you think? It still needs a section on data integrity/accuracy, but I'm not sure how to word it.

From: Chris Drake
To: Pack, Noah (POL)
Subject: Mobile & Fixed LPR Installation Guides
Date: Wednesday, April 6, 2022 4:00:37 PM
Attachments: L5F Fixed LPR installation Guide.docx
Vigilant Mobile ALPR Install Guide- DRAFT (1).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.

See Attached.

Chris Drake
Regional Sales Manager - New England
Video Security & Analytics
Vigilant Solutions

M: [redacted]

Support: (925) 398-2079 | Email Support

Follow LinkedIn

L6Q

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

From: Pack, Noah (POL)
To: Donnelly, William
Subject: MOU
Date: Saturday, May 28, 2022 9:39:00 AM
Attachments: ALPR TENANT MOU.docx
TRF-11 Nov21.pdf

Hi Bill,

Please see the attached MOU and our policy. Please let me know if you have any questions.

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: Pinkes, William (POL)
To: Ludlow AM (Michael Brennan)
Subject: MSP ALPR Policy
Date: Monday, March 7, 2022 2:56:00 PM
Attachments: TRF-11 ALPR Policy.pdf
image001.png

Hi Mike,

Attached is the current MSP ALPR policy. We do not have one on the use of tint meters. Hope this helps, should you have any questions or need anything further please reach out at your convenience.

Bill P.

Bill Pinkes
Accreditation Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-[redacted]

From: NFCA President
Subject: NFCA"s December Training Webinars Kickoff This Thursday with Globlue Technologies
Date: Monday, November 28, 2022 2:21:58 PM
Attachments: December 2022 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.

Please view the attached calendar to learn about the December training sessions offered by NFCA sponsors. The first of the December series takes place this Thursday, 12/1/2022 at 1:00 pm and is offered by Globlue Technologies. We conclude November's calendar with training by Fivecast on Tuesday at 1:00 pm EST.

The content developed for the NFCA training sessions is created for fusion centers and is focused on education. Our sponsors devote time and resources to create useful content, so please check out their sessions.

Thank you for supporting NFCA.

From: John Tedona
To: Pack, Noah (POL)
Cc: Cyrus Baldwin
Subject: P497 Installation Manual
Date: Monday, June 27, 2022 2:46:39 PM
Attachments: image001.png
image002.png
image003.png
PIPS Fixed Camera System Installation Guide_1-2018.pdf
P497 Overview.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,

At the moment you have the only P497 in the US….not even Cyrus has one yet. I'll check on the status of the installation manual; however aside from using a 18vdc nominal power supply it's wired up the same as a P492.

I've attached two pdfs are helpful until I get a finished copy of a P497 manual.

Feel free to email Cyrus (copied) for any assistance you may need in setting up the camera.

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

From: Egnitz, Brian D. (EPS)
To: Cyr, Mark (POL)
Subject: Policy
Date: Wednesday, December 7, 2022 5:16:09 PM
Attachments: Global Justice Public Safety Agreement FINAL 9-28-2020.docx

From: Pack, Noah (POL)
To: Staples, Jennifer (POL)
Cc: Brunelli, Daniel (POL)
Subject: RE: [External] RE: [EXTERNAL]ALPR TENANT MOU, with SPD proposed edits, and MSP General Order TRF-11
Date: Thursday, July 14, 2022 1:18:00 PM
Attachments: image001.png
GO 16-03 - ALPR Policy.doc
ALPR TENANT MOU, with SPD proposed edits.docx

Hi Jenn,

Sorry for the delay on this. Attached is the working version of our MOA with Springfield with their initial edits. Below is the latest email with the Springfield city solicitor's contact information if you need anything directly from them. Please let me know what else I can provide!

Dear Sgt. Pack/Noah:

I'm out of the office today, but I spoke with Bill Schwarz earlier and he told me you were at SPD to set up the access to the MSP ALPR.
A few weeks ago SPD Capt. Jeffrey Martucci (copied here) forwarded me the **SPD ALPR Policy** (attached). Is there a way to accommodate both policies in the MOU?
Bill said SPD can wait to start using the MSP system until this is worked out.
Sorry I didn't get back to you sooner- things are crazy busy these days with our fiscal year end. I can pick this back up next Tuesday 6/21 when I'm back in the office.

Best regards,
Kathy Breck 6/17/22

Kathleen T. Breck
Deputy City Solicitor
City of Springfield Law Department
36 Court Street, Room 210
Springfield, MA. 01103
(413)787-6179
kbreck@springfieldcityhall.com

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: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>

Sent: Monday, June 27, 2022 12:22 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Brunelli, Daniel (POL) <Daniel.Brunelli@pol.state.ma.us>
Subject: RE: [External] RE: [EXTERNAL]ALPR TENANT MOU, with SPD proposed edits, and MSP General Order TRF-11

Hello Sgt. Pack:

Legal has reviewed the Springfield City ALPR policy, and have no major concerns. However, the language to the MOA will need to be changed.

Can you forward the pending MOA with Springfield City to us and we can draft some proposed language for them to review which references their own policy.

Thanks!

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

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: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, June 21, 2022 3:09 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Cc: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>
Subject: FW: [External] RE: [EXTERNAL]ALPR TENANT MOU, with SPD proposed edits, and MSP General Order TRF-11

Hi Jenn,

Springfield City has responded to ask for further adjustments to the LPR MOU. They are now asking to incorporate their LPR policy (of which we were not previously aware) to the MOU. You can see the email from the city attorney below.

Any thoughts on this? For the sake of discussion, their policy does not look bad at all, but it would of course not reflect any future changes to ours. Sorry to be a broken record on this issue and thank you for your time.

Noah

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

From: Breck, Kathy <KBreck@springfieldcityhall.com>
Sent: Friday, June 17, 2022 2:58 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Schwarz, William J <WSchwarz@springfieldpolice.net>; Martucci, J <jmartucci@springfieldpolice.net>
Subject: FW: [External] RE: [EXTERNAL]ALPR TENANT MOU, with SPD proposed edits, and MSP General Order TRF-11

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.

Dear Sgt. Pack/Noah:

I'm out of the office today, but I spoke with Bill Schwarz earlier and he told me you were at SPD to set up the access to the MSP ALPR.
A few weeks ago SPD Capt. Jeffrey Martucci (copied here) forwarded me the **SPD ALPR Policy** (attached). Is there a way to accommodate both policies in the MOU?
Bill said SPD can wait to start using the MSP system until this is worked out.
Sorry I didn't get back to you sooner- things are crazy busy these days with our fiscal year end. I can pick this back up next Tuesday 6/21 when I'm back in the office.

Best regards,
Kathy Breck 6/17/22

Kathleen T. Breck
Deputy City Solicitor
City of Springfield Law Department
36 Court Street, Room 210
Springfield, MA. 01103
(413)787-6179
kbreck@springfieldcityhall.com

From: Sarasin, Ryan (CHS)
To: Cormier, Donald (POL)
Subject: RE: CJIS Agreement
Date: Friday, March 4, 2022 10:25:05 AM
Attachments: SP Framingham GHQ 01-12-2021.pdf
Global Justice Public Safety Agreement FINAL 9-28-2020.docx

Captain,

Attached is a copy of your most recent user agreement (not the global sharing agreement), but just your user agreement for CJIS.

That Global Sharing Agreement document that was attached is typically for the license plate readers, COPLINK, and a few others. I looked and it does not look like we have one of these on file for MSP. I am going to inquiry about whether we should moving forward, but right now it doesn't look like we do. I also attached a more recent Global Sharing Agreement that goes into a little more detail about the scope and need for the document.

Do you know what vendor (name) is asking for this document and the exact purpose. I understand they want to make sure you are authorized to access CJIS data. In my opinion, the user agreement does show you have the authority, I just want to confirm the vendor.

Thanks Captain!

-Ryan

From: Cormier, Donald (POL) <donald.cormier@pol.state.ma.us>
Sent: Thursday, March 3, 2022 10:30 PM
To: Sarasin, Ryan (CHS) <ryan.sarasin@mass.gov>
Subject: CJIS Agreement

Ryan,

Do you know where can I find this agreement? Above is a copy of something Sgt Pack attached to his original email to me. Thanks Capt. Cormier

Captain Donald J. Cormier #812

Massachusetts State Police

Division of Administrative Services

470 Worcester Rd.

Framingham, MA. 01702

(508) 820-2107

Email:donald.cormier@massmail.state.ma.us

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Thursday, March 3, 2022 2:29 PM
To: Cormier, Donald (POL) <donald.cormier@pol.state.ma.us>
Subject: CJIS Agreement

Captain Cormier,

Could you direct me to where I can find a copy of the Department's agreement with DCJIS to access CJIS data? I've attached the document I am referring to. We are working with a vendor who is looking for a copy for their files to ensure we are authorized to access CJIS data. Thank you.

From: Dumont, David M (POL)
To: Hutchinson, Daniel (CHS)
Subject: Re: CJIS REP Training
Date: Wednesday, October 26, 2022 7:54:13 AM
Attachments: CJIS-REP GUIDE .doc

Good Morning Dan,

Do you have an idea on how long you anticipate tomorrows training to be? Another Trooper and I are trying to figure out if we need to change our shift. Thank you -Dave

Respectfully,
Trooper David Dumont #3787
HSI, Task Force Officer
Massachusetts State Police
Division of Homeland Security & Preparedness
Fraud Identification Unit
185 Kneeland St, 5th Floor
Boston, MA 02111
Phone: 857-368-9500
Fax: 857-368-0649
David.Dumont@massmail.state.ma.us



CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. It may not be forwarded or further distributed without prior approval from the author. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call 857-368-9500 immediately. Thank you.*

> On Oct 13, 2022, at 11:24 AM, Hutchinson, Daniel (CHS) <daniel.hutchinson@mass.gov> wrote:
>
> Good Morning,
>
> I've attached a CJIS REP Guide for use during the training scheduled on Thursday, October 27th, 2022, 9:00a.m., at the MPTC located at 42 Thomas Petten Dr., Randolph, MA 02358. Please make a copy of the guide and bring it with you to the training. The CJIS Support Services Unit is looking forward to meeting everyone and providing this training. If you have any specific issues relating to CJIS that you have encountered and would like discussed send me a separate email so that I can research the issue prior to the training.
>
> Thank you,

Dan Hutchinson

[cid:image001.jpg@01D8DEF2.F60E64E0]
Daniel J. Hutchinson
Massachusetts Department of Criminal Justice Information Services
CJIS Support Services
200 Arlington Street-Suite 2200
Chelsea, MA 02150
F: 617-884-4601
Daniel.Hutchinson@<mailto:Daniel.Hutchinson@>mass.gov |
www.mass.gov/cjis<http://www.mass.gov/cjis>



From: Sarasin, Ryan (CHS)
To: Sullivan, Margaret (POL)
Subject: RE: DCJIS Forms
Date: Wednesday, April 27, 2022 12:07:39 PM
Attachments: Global Justice Public Safety Agreement FINAL 9-28-2020.docx

---

Good Morning,
Attached is the most recent Global Sharing Agreement. Once the Captain or someone at MSP signs, we can have our DCJIS Commissioner sign off.
-Ryan

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Tuesday, April 26, 2022 12:30 PM
To: Sarasin, Ryan (CHS) <ryan.sarasin@mass.gov>
Subject: FW: DCJIS Forms

Hi Ryan – Bill Dunn suggested I reach out to you to get a copy of the CJIS Global Sharing Agreement. From reading the attached email thread it appears to be related to an ALPR (license plate reader) vendor. Please let me know if you have questions or need additional information. Thank you for your assistance. -peg

Margaret Sullivan | Executive Office of Public Safety and Security
Director | Application Development and Support Services
Office of Technology and Information Services
470 Worcester Road
Framingham, MA 01702
p. 508-820-2227 | f. 508-820-2359

From: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Sent: Thursday, April 21, 2022 10:52 AM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Subject: RE: DCJIS Forms

I would suggest DCJIS Support (Next week) and ask for Ryan Sarasin
617 660 4710
However, there are a variety of those forms, based on slight differences/requirements
ALPR – License Plate Readers
Sharing RMS Cad
Regional Dispatch Centers
Fire Dept's / Non LE/CJ traversing the routers
Shared (Courtesy Booking) Live Scan
Hope this helps, although likely added more questions to the mix

---

From: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Sent: Thursday, April 21, 2022 10:46 AM
To: Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: DCJIS Forms

Hi Bill – I'm hoping you can assist in directing me to the appropriate person at DCJIS who can assist with getting a copy of the most recent version of the attached form. Any assistance you can provide is appreciated. Thanks. -peg

From: John Tedona
To: Pack, Noah (POL)
Subject: RE: Feature Request Update: Historical Search Time Limits and Device Visibility
Date: Monday, August 8, 2022 8:41:12 PM
Attachments: image001.png
image002.png
image003.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'm impressed. You are certainly an educated consumer. I'll make sure this gets notoriety on our roadmap.

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: Monday, August 8, 2022 8:30 PM
To: ALPR_Support <ALPR_Support@neology.net>; Michael Roth <mroth@neology.net>; Peter Crary <pcrary@neology.net>; Israel Padilla <ipadilla@neology.mx>
Cc: John Tedona <jtedona@neology.net>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Feature Request Update: Historical Search Time Limits and Device Visibility

Limit Historical Search Time

We are looking to restrict the amount of historical time that a user can search (ie, the full system retention or a lesser period, say 30 days). This feature request is coming up again because we are preparing to add dispatchers to the system, and we would prefer to restrict their access to a more limited time that is relevant to their duties. I think this makes the most sense to set at the group level (see attached) by selecting to enforce a historical search limit and then entering the allowable days, something similar to the hot plate expiration interface. This is a high priority for us.

Set Allowable Devices to See Results

-

We are still looking to restrict visibility of devices, including which devices a tenant can see results from. Currently, a searching user in any tenant will by default see results from every device in the system and can manually see and select from ALL devices from all other tenants using the device search filter. There is no apparent way to restrict this, as we discussed in the past during the earlier phase of our boss4 transition.

Ideally, the system should be set to allow administers to restrict cross-tenant visibility for devices or sites. This feature request is coming up again due to the addition of more local tenants to the system who we want to restrict to seeing just their own devices and search results from their own devices as opposed to the entire system. This feature is probably easiest to set at the agency/tenant level. This is a medium priority for us.

Why are these important?

Building in system level protections to manage user access to the amount and type of data that is relevant to their user group is an important step to protecting the integrity of the system and lowering the potential for accidental misuse.

Thank you. Please add to the agenda for our next update meeting.

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

To: Miller, Dianne (POL)
Subject: RE: FSHSP20CFC modification request
Date: Wednesday, September 28, 2022 12:24:04 PM
Attachments: image001.png
FSHSP20CFC FFY20 ISA POL CFC - ISA.doc

Hi Dianne:
Thanks – attached is the ISA moving items into equipment and UU.

I think the ALPR's and software are UU and the other is KK – do you agree?

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:53 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

I think she's decreasing AA and increasing UU.
So we need to make sure the UU total in column I adds up to what her quotes were for, and match her modification request letter.
Sorry, I didn't realize no carryforward was done. There's a spreadsheet in the V drive for carryforward so I assumed it was done.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:47 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
The carryforward has not been processed yet. They only did a blanket 90,000 back in June.

If we are carrying forward what was budgeted, I will re-work attachment B to adjust for the change in payroll tax, indirect, and fringe. Do you know if Amy wants to change any of the budgeted amounts in each category? I initially kept it blank as I didn't know if Amy wanted to adjust the categories.

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 10:45 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi again,
If a carryforward was already processed by EOPSS, then column E for FY22 would have the actual amounts you have in Column I.
And the amounts in column G are the starting point for FY23 in column E (for example, AA should have 10563.39, EE conference space should start with $5K in column E ….etc)
Unless I'm mistaken….I think that's how we would do it. Then add & subtract FY23 lines as needed to get to Amy's modified budget in column I.
Di

From: Miller, Dianne (POL)

Sent: Tuesday, September 27, 2022 4:31 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Questions…
Becky, attached is a carryforward that was already processed?
If yes, I think the carryforward amounts from column G are the starting point in column E for FY23….then show the increases and decreases that result in Column I amounts for Amy to spend down.

Amy…is this a good time to attach a food quote for the faith-based seminar and make sure it's approved? There's $5K for conference space, so maybe we can incorporate it all and make sure it's covered?
Vicky already has your equipment quotes so maybe it's not a good idea to attach another one. Just a thought.

[See Instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Am Afte Amendn
2022	8000-4692	AA	Salary	$59,133.39	-	$10563.39		$48570.00
2022	8000-4692	BB	Travel	$100,000	-	$94103.28		$5896.72
2022	8000-4692	CC	Contractor Services	$149,000	-	$73351.25		$75648.75
2022	8000-4692	DD	Payroll Tax @ $1.97%	$6198.31	-	$3572.04		$2626.27
2022	8000-4692	DD	Fringe @ 37.46%	$22151.37	-	$413.85		$18014.52
2022	8000-4692	EE	Indirect Cost @ 17.55%	$10377.91	-	$1853.86		$8524.05
2022	8000-4692	EE	Conference Space	$5000	-	$5000		$0
2022	8000-4692	EE	Supplies	$21467.5	+	$1548.50		$23016
2022	8000-4692	UU	IT Software	$120245.50	-	$120245.50		$0
2023	8000-4692	AA	Salary					
2023	8000-4692	BB	Travel					
2023	8000-4692	CC	Contractor Services	$106,426.02				
2023	8000-4692	DD	Payroll Tax @ $1.97%					
2023	8000-4692	DD	Fringe @ 37.46%					
2023	8000-4692	EE	Indirect Cost @ 17.55%					
2023	8000-4692	EE	Conference Space			$		$
2023	8000-4692	EE	Supplies			$		$
2023	8000-4692	UU	IT Software	$150,000.00				

Di

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 22, 2022 1:08 PM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Please see the completed Attachment A. Thank you both.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 2:00 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

The attachment B has been populated. I updated the FY22 numbers to match what is in MMARS. The total for FY22 is $186,296.31.

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?
Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division

10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Miller, Dianne (POL)
To: Rust, Rebecca (POL)
Subject: RE: FSHSP20CFC modification request
Date: Wednesday, September 28, 2022 11:52:00 AM
Attachments: FSHSP20CFC modification request.msg
Est_2524_from_BainCor_Inc._18968.pdf
FSHSP20CFC Modification Request August 2022.docx
image001.png

I think she's decreasing AA and increasing UU.
So we need to make sure the UU total in column I adds up to what her quotes were for, and match her modification request letter.
Sorry, I didn't realize no carryforward was done. There's a spreadsheet in the V drive for carryforward so I assumed it was done.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:47 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
The carryforward has not been processed yet. They only did a blanket 90,000 back in June.

If we are carrying forward what was budgeted, I will re-work attachment B to adjust for the change in payroll tax, indirect, and fringe. Do you know if Amy wants to change any of the budgeted amounts in each category? I initially kept it blank as I didn't know if Amy wanted to adjust the categories.

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 10:45 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi again,
If a carryforward was already processed by EOPSS, then column E for FY22 would have the actual amounts you have in Column I.
And the amounts in column G are the starting point for FY23 in column E (for example, AA should have 10563.39, EE conference space should start with $5K in column E ….etc)
Unless I'm mistaken….I think that's how we would do it. Then add & subtract FY23 lines as needed to get to Amy's modified budget in column I.
Di

From: Miller, Dianne (POL)
Sent: Tuesday, September 27, 2022 4:31 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Questions…
Becky, attached is a carryforward that was already processed?
If yes, I think the carryforward amounts from column G are the starting point in column E for FY23….then show the increases and decreases that result in Column I amounts for Amy to spend down.

Amy…is this a good time to attach a food quote for the faith-based seminar and make sure it's approved? There's $5K for

conference space, so maybe we can incorporate it all and make sure it's covered?
Vicky already has your equipment quotes so maybe it's not a good idea to attach another one. Just a thought.

[See instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Am Afte Amendn
2022	8000-4692	AA	Salary	$59,133.39	-	$10563.39		$48570.00
2022	8000-4692	BB	Travel	$100,000	-	$94103.28		$5896.72
2022	8000-4692	CC	Contractor Services	$149,000	-	$73351.25		$75648.75
2022	8000-4692	DD	Payroll Tax @ $1.97%	$6198.31	-	$3572.04		$2626.27
2022	8000-4692	DD	Fringe @ 37.46%	$22151.37	-	$413.85		$18014.52
2022	8000-4692	EE	Indirect Cost @ 17.55%	$10377.91	-	$1853.86		$8524.05
2022	8000-4692	EE	Conference Space	$5000	-	$5000		$0
2022	8000-4692	EE	Supplies	$21467.5	-	$1548.50		$23016
2022	8000-4692	UU	IT Software	$120245.50	-	$120245.50		$0
2023	8000-4692	AA	Salary					
2023	8000-4692	BB	Travel					
2023	8000-4692	CC	Contractor Services	$106,426.02				
2023	8000-4692	DD	Payroll Tax @ $1.97%					
2023	8000-4692	DD	Fringe @ 37.46%					
2023	8000-4692	EE	Indirect Cost @ 17.55%					
2023	8000-4692	EE	Conference Space			$		$
2023	8000-4692	EE	Supplies			$		$
2023	8000-4692	UU	IT Software	$150,000.00				

Di

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 22, 2022 1:08 PM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Please see the completed Attachment A. Thank you both.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 2:00 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

The attachment B has been populated. I updated the FY22 numbers to match what is in MMARS. The total for FY22 is $186,296.31.

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>

Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?
Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>

Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Rust, Rebecca (POL)
To: Miller, Dianne (POL)
Subject: RE: FSHSP20CFC modification request
Date: Wednesday, September 28, 2022 12:28:59 PM
Attachments: image001.png
FSHSP20CFC FFY20 ISA POL CFC - ISA.doc

Hi Dianne:
Thanks – attached is the ISA moving items into equipment and UU.

The Bain quote looks like KK and the software and ALPR's, UU – do you agree?

If so, can you double check the attached?

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:53 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

I think she's decreasing AA and increasing UU.
So we need to make sure the UU total in column I adds up to what her quotes were for, and match her modification request letter.
Sorry, I didn't realize no carryforward was done. There's a spreadsheet in the V drive for carryforward so I assumed it was done.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 11:47 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi Dianne:
The carryforward has not been processed yet. They only did a blanket 90,000 back in June.

If we are carrying forward what was budgeted, I will re-work attachment B to adjust for the change in payroll tax, indirect, and fringe. Do you know if Amy wants to change any of the budgeted amounts in each category? I initially kept it blank as I didn't know if Amy wanted to adjust the categories.

Becky

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 28, 2022 10:45 AM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Hi again,
If a carryforward was already processed by EOPSS, then column E for FY22 would have the actual amounts you have in Column I.

And the amounts in column G are the starting point for FY23 in column E (for example, AA should have 10563.39, EE conference space should start with $5K in column E ….etc)
Unless I'm mistaken….I think that's how we would do it. Then add & subtract FY23 lines as needed to get to Amy's modified budget in column I.
Di

From: Miller, Dianne (POL)
Sent: Tuesday, September 27, 2022 4:31 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Questions…
Becky, attached is a carryforward that was already processed?
If yes, I think the carryforward amounts from column G are the starting point in column E for FY23….then show the increases and decreases that result in Column I amounts for Amy to spend down.

Amy…is this a good time to attach a food quote for the faith-based seminar and make sure it's approved? There's $5K for conference space, so maybe we can incorporate it all and make sure it's covered?
Vicky already has your equipment quotes so maybe it's not a good idea to attach another one. Just a thought.

[See Instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Am After Amendn
2022	8000-4692	AA	Salary	$59,133.39	-	$10563.39		$48570.00
2022	8000-4692	BB	Travel	$100,000	-	$94103.28		$5896.72
2022	8000-4692	CC	Contractor Services	$149,000	-	$73351.25		$75648.75
2022	8000-4692	DD	Payroll Tax @ $1.97%	$6198.31	-	$3572.04		$2626.27
2022	8000-4692	DD	Fringe @ 37.46%	$22151.37	-	$413.85		$18014.52
2022	8000-4692	EE	Indirect Cost @ 17.55%	$10377.91	-	$1853.86		$8524.05
2022	8000-4692	EE	Conference Space	$5000	-	$5000		$0
2022	8000-4692	EE	Supplies	$21467.5	+	$1548.50		$23016
2022	8000-4692	UU	IT Software	$120245.50	-	$120245.50		$0
2023	8000-4692	AA	Salary					
2023	8000-4692	BB	Travel					
2023	8000-4692	CC	Contractor Services	$106,426.02				
2023	8000-4692	DD	Payroll Tax @ $1.97%					
2023	8000-4692	DD	Fringe @ 37.46%					
2023	8000-4692	EE	Indirect Cost @ 17.55%					
2023	8000-4692	EE	Conference Space			$		$
2023	8000-4692	EE	Supplies			$		$
2023	8000-4692	UU	IT Software	$150,000.00				

Di

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 22, 2022 1:08 PM
To: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Please see the completed Attachment A. Thank you both.

From: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 2:00 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>

Subject: RE: FSHSP20CFC modification request

The attachment B has been populated. I updated the FY22 numbers to match what is in MMARS. The total for FY22 is $186,296.31.

Becky

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:52 PM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: RE: FSHSP20CFC modification request

Thank you!

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Wednesday, September 21, 2022 1:22 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>
Subject: FW: FSHSP20CFC modification request

Hi Amy and Becky,
Usually I would do the attachment B and Amy would modify the language with red font and strikethroughs.
Right now, there is no language in there, so we need to copy and paste from the previous ISA.
Becky, did you want to do it or do you want me to?
Di

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Wednesday, September 21, 2022 1:20 PM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Attached, please find amended ISA for your action.

Thank you

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Tuesday, September 20, 2022 9:31 AM

To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hi Vicky,
Checking back on this request. Please let me know if you need any additional information. Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Sent: Thursday, September 1, 2022 8:33 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: FW: FSHSP20CFC modification request

Please disregard my email; I just saw the request
Apologies

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Mboka-Boyer, Vicky (OGR)
Sent: Thursday, September 1, 2022 8:31 AM
To: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Toner, Kayla (OGR) <Kayla.Toner@mass.gov>
Subject: RE: FSHSP20CFC modification request

Hello Melissa,

Thank you for the quotes for your budget modification request. Please provide me with a short narrative on these quotes.

Thank you again and I look forward to hearing from you.

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720 A
617-933-3530
Vicky.Mboka-Boyer@mass.gov

Sign up to receive notifications of grant opportunities from the Office of Grants and Research
https://www.mass.gov/forms/sign-up-to-receive-notifications-of-grant-opportunities-from-the-office-of-grants-and

---

From: Comeau, Melissa (POL) <Melissa.Comeau@pol.state.ma.us>
Sent: Thursday, August 25, 2022 9:22 AM
To: Mboka-Boyer, Vicky (OGR) <vicky.mboka-boyer@mass.gov>
Cc: Rust, Rebecca (POL) <Rebecca.Rust@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: FSHSP20CFC modification request

Hi Vicky,

I hope all is well! Please see attached modification request for FSHSP20CFC. We are also including quotes that support the costs.
Let me know if you need any additional information to approve this request.
Thank you.

Melissa Comeau
Director of Billing, Receivables & Grants
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Brooks, Brian (POL)
To: Bender, Sean (POL)
Subject: Re: Hotlists for Troop Dispatch
Date: Tuesday, August 30, 2022 9:04:56 AM
Attachments: image.png

Sean. I'll be in shortly. Yes I didn't reply till I had an opportunity to talk with you

Get Outlook for iOS

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, August 30, 2022 7:58:29 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>
Subject: Re: Hotlists for Troop Dispatch

Good Morning, Sir -

*Weighing in because Justin is off for a couple of days and Lt. Brooks is not in yet. I don't want you to think we're all ignoring your email!

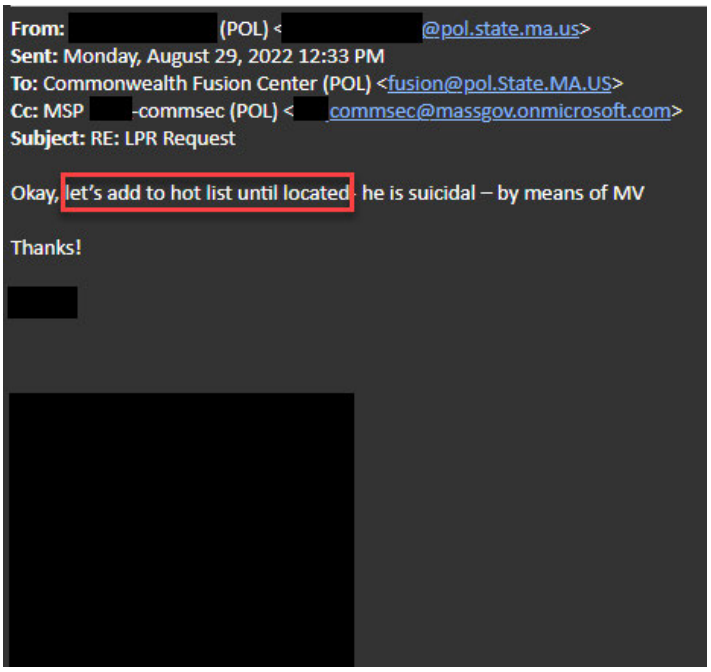
In looking through the plates currently in the various Troop Dispatch hotlists, it looks like most folks are generally utilizing the default expiration date when entering a plate. I will send out a reminder to our Analytical Staff to exercise some discretion/common sense when entering hotlists for Dispatch BOLOs.

As you are aware, some of the Troop Dispatch centers have developed strong opinions about the appropriate usage of the ALPR system. I certainly agree that in a perfect world, our Analytical Staff would be able to exercise 'best judgement' in setting hotlist expiration dates, and a written policy would go a long way towards giving us some leverage to push back on requests that don't meet whatever threshold is decided on.

An example we received yesterday:

Missing / Potentially Q5 Party

- 12:29 - Request from Troop Dispatch for historical data
- 12:31 - CFC Response: No hits within past 24 hours
- 12:33 - Request from Troop Dispatch for hotlist (see below):


From: [redacted] (POL) <[redacted]@pol.state.ma.us>
Sent: Monday, August 29, 2022 12:33 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: MSP [redacted]-commsec (POL) <[redacted]commsec@massgov.onmicrosoft.com>
Subject: RE: LPR Request

Okay, let's add to hot list until located - he is suicidal – by means of MV

Thanks!

[redacted]

[redacted]

- 12:37 - After discussion between myself and the Analyst handling the request, we settled on a hotlist for 24 hours with the justification that if 24 hours pass, the party will likely either be located, or the Q5 risk will have been mitigated/unsubstantiated.
- 13:15 - Subject located.

In this case, the requestor asked for a hotlist 'until the subject is located'. TTL in this case ended up being less than an hour, so there was absolutely no need for a 30 day hotlist and 24 hours ended up being *more* than sufficient, possibly even still excessive.

My issue with a request like this is that we are trying to balance accommodating the requestor while also exercising an appropriate level of discretion. Without a written policy to cite, we don't have a lot of protection with which to push back, as evidenced by some of our recent issues and complaints we have received with the level of assistance rendered. We put that Q5 plate on a 24 hour hotlist. If that hotlist expires and the party hits on the LPR at hour 25 and kills themselves or somebody else at hour 26, we're in the glue because the requestor asked for a longer date and we exercised discretion to overrule them.

In absence of an updated written policy a la TRF-11, I think it would be very beneficial to have some of the Dispatch Centers who want to utilize the LPR system either directly or through the CFC, receive some training on authorized/appropriate usage and/or guidelines for submitting LPR requests.

Respectfully,

Sean Bender
Intelligence Analyst

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, August 27, 2022 7:48 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>; Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: Hotlists for Troop Dispatch

Sirs:

We are working on training and guidelines for dispatchers regarding LPR, and I'm looking for your feedback. At present, when a troop dispatch asks to put a license plate on a hotlist, please vet the reason for the entry and select the expiration date accordingly. (Do you do this now, or do you generally just enter it for the default period?) In many cases, such as when entering BOLOs or info for agencies reporting a real time event, **hotlist entry expiration of 24 hours or less is likely appropriate.** Recall that the default expiration date is 30 days unless adjusted when entering the plate. Leaving a stale BOLO in a dispatch hotlist, which could result in a broadcast to Troopers when the vehicle is no longer wanted or sought, is a situation we seek to avoid.

Example 1: a BOLO is put out for a vehicle involved in a shooting in Springfield. This matter will be investigated by Springfield PD, and they have access to the LPR system or can contact CFC/CWC directly to use it in their investigation. The active life of this BOLO is probably not more than a few hours or end of the working crew's shift, unless circumstances dictate otherwise.

Information changes quickly, and it is the responsibility (by policy) of the members entering or requesting the entries to remove them when no longer needed. It is not the duty of our dispatchers to stay abreast of ongoing investigations. Since they may be unaware if a plate needs to stay on the hotlist, it follows that they generally should not be requesting hotlist entries for an extended period of time.

Example 2: Brockton PD broadcasts info on a recently stolen vehicle. This vehicle hasn't yet been entered into NCIC. The active life of this BOLO is also probably not more than a few hours or end of the working crew's shift. The vehicle will be entered into NCIC (and removed by the ORI when no longer stolen). Manual hotlist entries are not intended to serve as a long term means to identify and broadcast motor vehicle offenses over troop radios.

Please let know your thoughts on this, including any other common scenarios you find when field inquiries from dispatch. Once we get the appropriate guidelines here, we can push it out to your team and to the dispatchers in their training.

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: Bender, Sean (POL)
To: Pack, Noah (POL)
Cc: Brooks, Brian (POL); Salvatore, Justin (POL)
Subject: Re: Hotlists for Troop Dispatch
Date: Tuesday, August 30, 2022 7:58:32 AM
Attachments: image.png

Good Morning, Sir -

*Weighing in because Justin is off for a couple of days and Lt. Brooks is not in yet. I don't want you to think we're all ignoring your email!

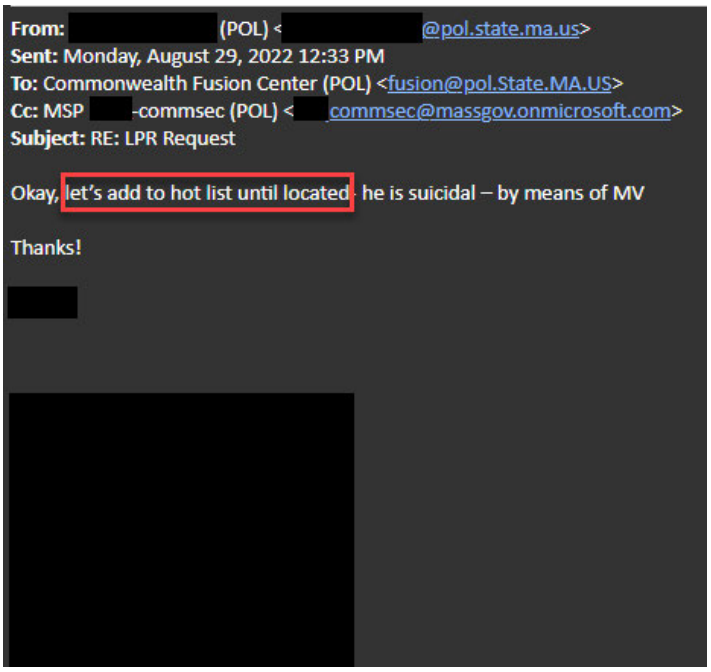
In looking through the plates currently in the various Troop Dispatch hotlists, it looks like most folks are generally utilizing the default expiration date when entering a plate. I will send out a reminder to our Analytical Staff to exercise some discretion/common sense when entering hotlists for Dispatch BOLOs.

As you are aware, some of the Troop Dispatch centers have developed strong opinions about the appropriate usage of the ALPR system. I certainly agree that in a perfect world, our Analytical Staff would be able to exercise 'best judgement' in setting hotlist expiration dates, and a written policy would go a long way towards giving us some leverage to push back on requests that don't meet whatever threshold is decided on.

An example we received yesterday:

Missing / Potentially Q5 Party

- 12:29 - Request from Troop Dispatch for historical data
- 12:31 - CFC Response: No hits within past 24 hours
- 12:33 - Request from Troop Dispatch for hotlist (see below):



- 12:37 - After discussion between myself and the Analyst handling the request, we settled on a hotlist for 24 hours with the justification that if 24 hours pass, the party will likely either be located, or the Q5 risk will have been mitigated/unsubstantiated.
- 13:15 - Subject located.

In this case, the requestor asked for a hotlist 'until the subject is located'. TTL in this case ended up being less than an hour, so there was absolutely no need for a 30 day hotlist and 24 hours ended up being *more* than sufficient, possibly even still excessive.

My issue with a request like this is that we are trying to balance accommodating the requestor while also exercising an appropriate level of discretion. Without a written policy to cite, we don't have a lot of protection with which to push back, as evidenced by some of our recent issues and complaints we have received with the level of assistance rendered. We put that Q5 plate on a 24 hour hotlist. If that hotlist expires and the party hits on the LPR at hour 25 and kills themselves or somebody else at hour 26, we're in the glue because the requestor asked for a longer date and we exercised discretion to overrule them.

In absence of an updated written policy a la TRF-11, I think it would be very beneficial to have some of the Dispatch Centers who want to utilize the LPR system either directly or through the CFC, receive some training on authorized/appropriate usage and/or guidelines for submitting LPR requests.

Respectfully,

Sean Bender
Intelligence Analyst

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, August 27, 2022 7:48 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>; Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: Hotlists for Troop Dispatch

Sirs:

We are working on training and guidelines for dispatchers regarding LPR, and I'm looking for your feedback. At present, when a troop dispatch asks to put a license plate on a hotlist, please vet the reason for the entry and select the expiration date accordingly. (Do you do this now, or do you generally just enter it for the default period?) In many cases, such as when entering BOLOs or info for agencies reporting a real time event, **hotlist entry expiration of 24 hours or less is likely appropriate.** Recall that the default expiration date is 30 days unless adjusted when entering the plate. Leaving a stale BOLO in a dispatch hotlist, which could result in a broadcast to Troopers when the vehicle is no longer wanted or sought, is a situation we seek to avoid.

Example 1: a BOLO is put out for a vehicle involved in a shooting in Springfield. This matter will be investigated by Springfield PD, and they have access to the LPR system or can contact CFC/CWC directly to use it in their investigation. The active life of this BOLO is probably not more than a few hours or end of the working crew's shift, unless circumstances dictate otherwise.

Information changes quickly, and it is the responsibility (by policy) of the members entering or requesting the entries to remove them when no longer needed. It is not the duty of our dispatchers to stay abreast of ongoing investigations. Since they may be unaware if a plate needs to stay on the hotlist, it follows that they generally should not be requesting hotlist entries for an extended period of time.

Example 2: Brockton PD broadcasts info on a recently stolen vehicle. This vehicle hasn't yet been entered into NCIC. The active life of this BOLO is also probably not more than a few hours or end of the working crew's shift. The vehicle will be entered into NCIC (and removed by the ORI when no longer stolen). Manual hotlist entries are not intended to serve as a long term means to identify and broadcast motor vehicle offenses over troop radios.

Please let know your thoughts on this, including any other common scenarios you find when field inquiries from dispatch. Once we get the appropriate guidelines here, we can push it out to your team and to the dispatchers in their training.

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: Tucker, Daniel T (POL)
To: Brooks, Brian (POL)
Subject: Re: Hotlists for Troop Dispatch
Date: Tuesday, August 30, 2022 8:48:54 PM
Attachments: image.png
image001.png

Hi Brian,

Lets talk tomorrow about this.

Thanks

Major Daniel T Tucker #2938
Massachusetts State Police
Division of Homeland Security and Preparedness
Deputy Division Commander - CIIS
(office) 978-451-3754
(cell) 781-[redacted]

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, August 30, 2022 2:05 PM
To: Tucker, Daniel T (POL) <Daniel.T.Tucker@pol.state.ma.us>
Subject: FW: Hotlists for Troop Dispatch

Major, please see IA Bender's response below in which I think he makes excellent points. Before I respond to Sgt. Pack, I'd like to discuss with you Sgt. Packs suggestions. Respectfully, Brian

Lieutenant Brian Brooks
Commonwealth Fusion Center – Watch Center
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2233

From: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Sent: Tuesday, August 30, 2022 7:58 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL)

<Justin.Salvatore@pol.state.ma.us>
Subject: Re: Hotlists for Troop Dispatch

Good Morning, Sir -

*Weighing in because Justin is off for a couple of days and Lt. Brooks is not in yet. I don't want you to think we're all ignoring your email!

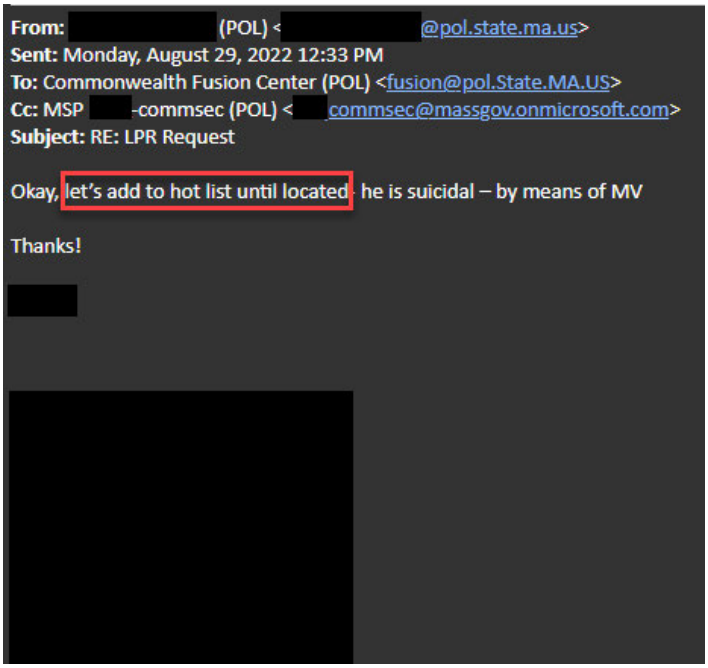
In looking through the plates currently in the various Troop Dispatch hotlists, it looks like most folks are generally utilizing the default expiration date when entering a plate. I will send out a reminder to our Analytical Staff to exercise some discretion/common sense when entering hotlists for Dispatch BOLOs.

As you are aware, some of the Troop Dispatch centers have developed strong opinions about the appropriate usage of the ALPR system. I certainly agree that in a perfect world, our Analytical Staff would be able to exercise 'best judgement' in setting hotlist expiration dates, and a written policy would go a long way towards giving us some leverage to push back on requests that don't meet whatever threshold is decided on.

An example we received yesterday:

Missing / Potentially Q5 Party

- 12:29 - Request from Troop Dispatch for historical data
- 12:31 - CFC Response: No hits within past 24 hours
- 12:33 - Request from Troop Dispatch for hotlist (see below):



12:37 - After discussion between myself and the Analyst handling the request, we settled on a hotlist for 24 hours with the justification that if 24 hours pass, the party will likely either be located, or the Q5 risk will have been mitigated/unsubstantiated.

- 13:15 - Subject located.

In this case, the requestor asked for a hotlist 'until the subject is located'. TTL in this case ended up being less than an hour, so there was absolutely no need for a 30 day hotlist and 24 hours ended up being *more* than sufficient, possibly even still excessive.

My issue with a request like this is that we are trying to balance accommodating the requestor while also exercising an appropriate level of discretion. Without a written policy to cite, we don't have a lot of protection with which to push back, as evidenced by some of our recent issues and complaints we have received with the level of assistance rendered. We put that Q5 plate on a 24 hour hotlist. If that hotlist expires and the party hits on the LPR at hour 25 and kills themselves or somebody else at hour 26, we're in the glue because the requestor asked for a longer date and we exercised discretion to overrule them.

In absence of an updated written policy a la TRF-11, I think it would be very beneficial to have some of the Dispatch Centers who want to utilize the LPR system either directly or through the CFC, receive some training on authorized/appropriate usage and/or guidelines for submitting LPR requests.

Respectfully,

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

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Saturday, August 27, 2022 7:48 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>; Salvatore, Justin (POL) <Justin.Salvatore@pol.state.ma.us>; Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: Hotlists for Troop Dispatch

Sirs:

We are working on training and guidelines for dispatchers regarding LPR, and I'm looking for your feedback. At present, when a troop dispatch asks to put a license plate on a hotlist, please vet the reason for the entry and select the expiration date accordingly. (Do you do this now, or do you generally just enter it for the default period?) In many cases, such as when entering BOLOs or info for agencies reporting a real time event, **hotlist entry expiration of 24 hours or less is likely appropriate.** Recall that the default expiration date is 30 days unless adjusted when entering the

plate. Leaving a stale BOLO in a dispatch hotlist, which could result in a broadcast to Troopers when the vehicle is no longer wanted or sought, is a situation we seek to avoid.

Example 1: a BOLO is put out for a vehicle involved in a shooting in Springfield. This matter will be investigated by Springfield PD, and they have access to the LPR system or can contact CFC/CWC directly to use it in their investigation. The active life of this BOLO is probably not more than a few hours or end of the working crew's shift, unless circumstances dictate otherwise.

Information changes quickly, and it is the responsibility (by policy) of the members entering or requesting the entries to remove them when no longer needed. It is not the duty of our dispatchers to stay abreast of ongoing investigations. Since they may be unaware if a plate needs to stay on the hotlist, it follows that they generally should not be requesting hotlist entries for an extended period of time.

Example 2: Brockton PD broadcasts info on a recently stolen vehicle. This vehicle hasn't yet been entered into NCIC. The active life of this BOLO is also probably not more than a few hours or end of the working crew's shift. The vehicle will be entered into NCIC (and removed by the ORI when no longer stolen). Manual hotlist entries are not intended to serve as a long term means to identify and broadcast motor vehicle offenses over troop radios.

Please let know your thoughts on this, including any other common scenarios you find when field inquiries from dispatch. Once we get the appropriate guidelines here, we can push it out to your team and to the dispatchers in their training.

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: Commonwealth Fusion Center (POL)
To: Smith, Eleanor (POL)
Cc: Salvatore, Justin (POL)
Subject: Re: Idi Investigative Platform
Date: Thursday, June 2, 2022 11:35:33 AM
Attachments: image001.png
LawEnforcementFusionCenter_CaseStudy.pdf
idiCORE.pdf

Good Morning!

I saw that Justin had forwarded this while I was going catching up to speed on last night. I was actually able to test idiCORE as part of a trial a few years back. It's very similar to CLEAR/TLO (and presumably Accurint/LexisNexus), and if memory serves, the company was actually started by persons who worked on TLO.

The database was pretty new when we tested it, but it did seem pretty good, especially with phone numbers, which seems to be the crux of their pitch.

Sgt. Noah Pack, who is now the ALPR Coordinator, was actually the one who I believe spearheaded the Department's trial, if anyone has any questions about it or was interested in looking into it further.

Respectfully,

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

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

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Wednesday, June 1, 2022 4:29 PM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: Fw: Idi Investigative Platform

Elly,

I am not familiar with this product. Just sending it along as an FYI.

Respectfully,

Justin Salvatore
Intelligence Analyst II

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

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

From: Omari Moench <omoench@ididata.com>
Sent: Wednesday, June 1, 2022 3:29 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Idi Investigative Platform

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.

Marci,

Great speaking with you.

I'd like to extend an invitation to a **free 30-day pilot** of our investigative platform. With unlimited users & unlimited searches

We are a 100% cloud native platform, with some of the most accurate phone numbers, criminal information & addresses.

Either way our job only works by making yours easier and with this platform I truly believe we can help close some pending cases at a higher rate with the data we are able to provide for law enforcement and FC's

Thank you for your time & service.

Looking forward to hearing from you.

Omari Moench | Account Executive
IDI, a red violet company (NASDAQ: RDVT)
2650 N. Military Trail, Suite 300
Boca Raton, FL 33431
561-757-4592 Direct
855-842-1410 Toll Free
561-336-0025 Fax

From: John Robling
To: Pack, Noah (POL)
Subject: Re: Introduction
Date: Thursday, May 26, 2022 8:11:12 AM
Attachments: Rekor Edge Max - Spec 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.

Hi Patrick,

I believe I can get you a trail license issued for that with no issues.

I apologize for the delay and confusion we have gone through some changes that will allow us to demonstrate the software much easier.

We have also rolled out some lease pricing starting at $1,800 per camera, per year.

Would 30 days suffice?
Should the license be registered to your email?

Best,
John

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Wednesday, May 25, 2022 12:52 PM
To: John Robling <jrobling@rekor.ai>
Subject: RE: Introduction

Hi John,

We have been exploring the options provided by several vendors. As I recall, you indicated that Rekor was not willing to send us a demo unit unless we essentially committed to purchase afterwards. When I asked for a trial license to test the software, you told me to sign up online for the two-week trial and suggested that extending it beyond that would be difficult.

While this is markedly unhelpful, I attempted to sign up for a trial account anyways. However, the website does not present the option to select the trial option with Axis camera integration and is asking for a credit card to activate the trial.

If Rekor wishes to allow us to demo this hardware or software, please advise.

Sincerely,

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 Robling <jrobling@rekor.ai>
Sent: Thursday, March 10, 2022 12:50 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Introduction

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 hope you are doing well. I wanted to circle back with you and see if you still had interest in our LPR cameras and if there is anything I can do to be a resource for you?

Best,
John

From: John Robling <jrobling@rekor.ai>
Sent: Wednesday, January 5, 2022 10:42 AM
To: Pack, Noah (POL) <noah.pack@state.ma.us>
Subject: Re: Introduction

Hi Noah,

I hope you had a great Christmas and New Year. I wanted to follow up to our meeting and see if you had any other questions or feedback?

Please let me know if there is anything I can do to assist you.

Best,
John

From: John Robling <jrobling@rekor.ai>
Sent: Monday, December 20, 2021 9:18 AM
To: Pack, Noah (POL) <noah.pack@state.ma.us>
Subject: Re: Introduction

Morning Noah,

I believe when moving the camera you would just need to update the GPS coordinates of the camera.
I will double check with my engineering department and confirm.

We do offer the ability to purchase as well. We understand that grants sometimes have stipulations. We are happy to work with you on those weather it is a purchase or a extended lease model.
Does the grant allow you to pay for SaaS services? In the currently model you do not of own the hardware you are just paying for the service I am not sure how that would affect the grant. Happy to discuss all options with you.

Purchasing 1 of the edge cameras would look roughly like this below. About 15K to own the hardware and have 5 years of service.

Edge300 - $6,950
5 YR Scout License $2,400
5-YR 4G LTE Communications $4,500
Install $500
Travel $750

Versus our Saas Model would be $6,000 over 5 years, per camera, and you don't have to maintain the hardware.

Happy to hop on a call this week to discuss if you would like.

Best,
John

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Friday, December 17, 2021 4:54 PM
To: John Robling <jrobling@rekor.ai>
Subject: Re: Introduction

Hi John,

Thanks for your time yesterday. Our team discussed this today, and we have a couple follow-up questions for you.

Some of our cameras are moved intermittently, at which time we update the location in the system for that camera. I understand that one of the reasons we could not go with Rekor in

the past was that the Rekor software cannot accurately accommodate these changes. Specifically, if Camera A is at Location A for July, then Camera A is at Location B for August, the system must be able to accurately reflect that history. It must not then appear that reads captured by Camera A in July were at Location B just because the camera was later moved there. Can you find out if this problem has been corrected and camera reads shows accurate historical locations even if devices are moved?

Additionally, as I'm sure you know, many LPR systems are purchased with grant funding. Grant funding is not ideal for subscription based services, as grants generally cannot be used to pay for subscriptions that run past the end of the grant period. Does Rekor have a sales package that accommodates this, such as buying the cameras/services outright?

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 Robling <jrobling@rekor.ai>
Sent: Monday, December 13, 2021 1:00 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Introduction

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.

2 Pm works. I will send a calendar invite.

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Monday, December 13, 2021 12:39 PM
To: John Robling <jrobling@rekor.ai>
Subject: Re: Introduction

Hi John, I have a court event that morning. Could we go for afternoon, say 2pm +/-?

Respectfully,

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 Robling <jrobling@rekor.ai>
Sent: Monday, December 13, 2021 9:48:59 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Introduction

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,

How's is 10 or 11 am on Thursday?

Best,
John

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Wednesday, December 8, 2021 8:21 PM
To: John Robling <jrobling@rekor.ai>
Subject: Re: Introduction

Sorry to hear that, hope you are feeling alright. I can do next Thursday, I will just have to get back to you once I have another time pinned down.

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 Robling <jrobling@rekor.ai>
Sent: Wednesday, December 8, 2021 12:00 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: Re: Introduction

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,

Great to hear from you. Yes that is correct. I am your new point of contact. I would be happy to assist you in any way I can.

I am out sick this week with Covid. Can we schedule 20-30 minutes next Tues, Wed, or Thursday?

Best,
John

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Wednesday, December 8, 2021 11:48 AM
To: John Robling <jrobling@rekor.ai>
Subject: Introduction

Hi John,

I have recently taken over as the ALPR administrator for the Massachusetts State Police. I had spoken previously with Gregg Williams, but I understand you may be our new regional sales rep. I'd like to open a line of contact with you as we move forward.

In the near future, I'm interested in testing some of your offerings, possibly including a fixed edge camera, mobile unit, and watchman software running over a cruiser camera. I look forward to touching base soon.

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

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.

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.

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.

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: Monahan, Meagen (NFK)
To: Connor, Greg (NFK); Tully, Brian (NFK)
Cc: Dicicco, David M (POL)
Subject: RE: Jeep SW
Date: Friday, August 26, 2022 8:52:56 AM
Attachments: 3 - Commonwealth v McCarthy.pdf
1 - Commonwealth v Henley.pdf

Before pulling additional video and LPR, I want to just check in on the net we are casting and whether it would be better served down the road to get SWs for these cameras/videos which would then be the basis for our SWs going forward.

I have concerns with the language in McCarthy (attached) about how the Court wished the record was more developed as to how many cameras MSP had and how many of those cameras recorded the car. The Court implied this could impact their analysis in the future, but resolved the case on the record before them which only had 4 cameras. Henley (the MBTA card case) seems to suggest it is the data we ultimately search and seize. But I want to air on the side of caution given McCarthy is about ALPR.

I am in the office at x4867 and my cell is [redacted].

Meagen K. Monahan
Assistant District Attorney
Norfolk District Attorney's Office
45 Shawmut Road
Canton, Massachusetts 02021
781-830-4800
781-830-4801 (fax)
781-562-0834 (shared efax)
meagen.monahan@massmail.state.ma.us

NOTICE: *This e-mail message may contain information that is confidential, proprietary and/or privileged. If you have received this transmission in error, please notify the sender immediately by return e-mail and destroy the original message and all copies.*

From: Connor, Greg (NFK) <Greg.Connor@MassMail.State.MA.US>
Sent: Friday, August 26, 2022 8:01 AM
To: Tully, Brian (NFK) <Brian.P.Tully@MassMail.State.MA.US>
Cc: Dicicco, David M (POL) <David.M.Dicicco@pol.state.ma.us>; Monahan, Meagen (NFK) <Meagen.Monahan@mass.gov>
Subject: Re: Jeep SW

Is there any video from [redacted]) during this time frame showing his car leave? Would it also show his car in the parking lit? This would confirm that it is not there.

On Aug 25, 2022, at 9:21 PM, Tully, Brian (NFK) <Brian.P.Tully@massmail.state.ma.us> wrote:

Attached is SW to seize and search the Jeep Cherokee.

DLt. Brian Tully #3520
Norfolk County State Police Detective Unit
Massachusetts State Police
781-830-4992
(f) 781-251-0750

From: Sonia, Michael (POL)
To: Reagan Thomas J; TED MINALL; White Paul
Cc: Landi Jeffrey; Ruggiero Paul; Beauchamp Roger; Richard.sullivan@risp.gov; Jenkins Bill
Subject: RE: LEL Meeting
Date: Thursday, June 16, 2022 10:03:00 AM
Attachments: TrafficSafety Report.pdf
image005.png

I didn't know if anyone had access to the IACP info so I attached their big resource book. I'm going to find out if there is a head of traffic safety at the IACP. I'd like to see studies rather than what people think is going on.

I think a survey to the Chiefs would be good start.

I think we need to remind officers who important traffic stops are as a preventative to poor behavior. We show a MADD video at our BT classes. One of the victims talks about an officer that pulled an OUI over and had him sleep it off. He left several minutes later and killed her daughter. We are trying to put in the minds of the officer that traffic safety makes a difference.

From: Reagan, Thomas J <Thomas.J.Reagan@maine.gov>
Sent: Thursday, June 16, 2022 9:50 AM
To: TED MINALL <tedbb@aol.com>; White, Paul <Paul.White@vermont.gov>
Cc: Landi, Jeffrey <Jeffrey.A.Landi@dos.nh.gov>; Sonia, Michael (POL) <michael.sonia@pol.state.ma.us>; Ruggiero, Paul <Paul.P.Ruggiero@dos.nh.gov>; Beauchamp, Roger <Roger.R.Beauchamp@dos.nh.gov>; Richard.sullivan@risp.gov; Jenkins, Bill <Bill.Jenkins@partner.vermont.gov>
Subject: RE: LEL 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.

Just a thought.
Many chiefs go through the FBI Academy in Quantico, Virginia. I wonder if traffic safety is even mentioned. That might be a good start teaching administrators and stressing DDACTs and the benefits of traffic safety.
Tom

From: TED MINALL <tedbb@aol.com>
Sent: Thursday, June 16, 2022 9:43 AM
To: White, Paul <Paul.White@vermont.gov>
Cc: Landi, Jeffrey <Jeffrey.A.Landi@dos.nh.gov>; Reagan, Thomas J <Thomas.J.Reagan@maine.gov>; Michael.sonia@pol.state.ma.us; Ruggiero, Paul <Paul.P.Ruggiero@dos.nh.gov>; Beauchamp, Roger <Roger.R.Beauchamp@dos.nh.gov>; Richard.sullivan@risp.gov; Jenkins, Bill <Bill.Jenkins@partner.vermont.gov>
Subject: Re: LEL Meeting

EXTERNAL: This email originated from outside of the State of Maine Mail System. Do not click links or open attachments unless you recognize the sender and know the content is safe.
Hey Jeff, I'm on the road conducting DRE candidate interviews. I know you're off on Fridays. I'll give you a call on Monday. Enjoy the weekend.

Sent from Ted's IPhone

> On Jun 16, 2022, at 9:30 AM, White, Paul <Paul.White@vermont.gov> wrote:
>
> Good morning all,

I will add to Jeff's list of reasons for waning enforcement.

It is curious to see that in NH, the SP is still carrying the load. That always used to be the case here in VT as well, before COVID came along. Now I would say that for the past two years it is the sheriffs' departments and a handful of local PDs that are carrying the load. ***In my opinion***, VSP leadership used COVID as an excuse to take a step back away from doing motor vehicle work for public health reasons but also as an opportunity to re-evaluate whether motor vehicle work is "worth the risk" (my words) of a potential bad outcome if some trooper somewhere has a bad stop and creates another national headline. Add to that the fact that none of the top commanders at VSP were ever strong "motor vehicle guys" in the early years of their respective careers, motor vehicle work is no longer made to be a priority in the department. And, we have many local PDs that will always follow VSP's lead... if the troopers aren't stopping cars then these local officers aren't going to stop them either. So now we have two years' worth of new hires that have come into the profession in an environment where motor vehicle work is not only not a priority, but outright frowned upon in some cases. We're going to have a very hard time to turn this ship around now.

Paul

Paul White, Law Enforcement Liaison
Vermont State Highway Safety Office
2178 Airport Road (Berlin)
Barre, VT 05641

Ph.: (802) 522-7529
E: Paul.White@vermont.gov

From: Landi, Jeffrey <Jeffrey.A.Landi@DOS.NH.GOV>
Sent: Thursday, June 16, 2022 8:40 AM
To: Reagan, Thomas J <Thomas.J.Reagan@maine.gov>; Ted Minall <tedbb@aol.com>; michael.sonia@pol.state.ma.us; Ruggiero, Paul <Paul.P.Ruggiero@DOS.NH.GOV>; Beauchamp, Roger <Roger.R.Beauchamp@DOS.NH.GOV>; richard.sullivan@risp.gov; Jenkins, Bill <Bill.Jenkins@partner.vermont.gov>; White, Paul <Paul.White@vermont.gov>
Subject: RE: LEL Meeting

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.
Hi Tom,

We see it here too. We get very little effort for the money spent with most local PDs and the SP carries the load. If it weren't for share to local, we could be much more effective in our enforcement efforts.

SECTION 402 REQUIREMENTS:

4. At least 40 percent of all Federal funds apportioned to this State under 23 U.S.C. 402 for this fiscal year will be expended by or for the benefit of political subdivisions of the State in carrying out local highway safety programs (23 U.S.C. 402(b)(1)(C)) or 95 percent by and for the benefit of Indian tribes (23 U.S.C. 402(h)(2)), unless this requirement is waived in writing. (This provision is not applicable to the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.)

That said, as we have discussed here, it would be better for the state of New Hampshire, and other states as well I am sure if, "will be **expended** by or for the benefit of", read "will be **allocated** to, for the benefit of" political subdivisions of the state. And not have it held against the state if those allocations were not

spent by those political subdivisions, as is currently the case.

Some reasons for waning enforcement, as I see it, for discussion:

1. Share to Local requirements/Poor Local PD effort
2. Negative media attention
3. Eroding political support from the top down
4. Public indifference
5. Poor generational work ethics
6. Recruitment difficulties/staffing problems
7. Lack of strong PD leadership/cautious leadership given 2 through 5.

Sorry for the rant. Have a great day!

Jeff



#GetHomeSafely
#CrashNotAccident

Jeffrey A. Landi
Law Enforcement Liaison/State Contracts
New Hampshire Department of Safety
33 Hazen Drive Room 208
Concord, NH 03305
Office: 603-271-2131
Direct: 603-271-6709
Email: jeffrey.landi@dos.nh.gov

Highway Safety Media Toolbox: https://www.trafficsafetymarketing.gov/

This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by law. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited and may be subject to criminal prosecution. If you have received this e-mail in error, please immediately notify me by telephone at (603) 271-2131.

From: Reagan, Thomas J <Thomas.J.Reagan@maine.gov>
Sent: Thursday, June 16, 2022 8:17 AM
To: Landi, Jeffrey <Jeffrey.A.Landi@DOS.NH.GOV>; Ted Minall <tedbb@aol.com>; michael.sonia@pol.state.ma.us; Ruggiero, Paul <Paul.P.Ruggiero@DOS.NH.GOV>; Beauchamp, Roger <Roger.R.Beauchamp@DOS.NH.GOV>; richard.sullivan@risp.gov; bill.jenkins@partner.vermont.gov; paul.white@vermont.gov
Subject: LEL Meeting

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

And another day passes with an additional fatality in Maine.

Great rant Jeff.

Topic for the meeting: Why is enforcement still down? We've blamed it on a new generation but there has to be more to it. We need to list all the reasons then discuss which ones we can successfully

address.

During a meeting yesterday I learned the 36 agencies using eCitations wrote 55% of the traffic violations this year, 10,327. That means the other 90 or so agencies wrote 45%.

Tom

From: Landi, Jeffrey <Jeffrey.A.Landi@DOS.NH.GOV>
Sent: Thursday, June 16, 2022 7:42 AM
To: Ted Minall <tedbb@aol.com>; Reagan, Thomas J <Thomas.J.Reagan@maine.gov>; michael.sonia@pol.state.ma.us; Ruggiero, Paul <Paul.P.Ruggiero@DOS.NH.GOV>; Beauchamp, Roger <Roger.R.Beauchamp@DOS.NH.GOV>; richard.sullivan@risp.gov; bill.jenkins@partner.vermont.gov; paul.white@vermont.gov
Subject: RE: [Dps.alldre] Motor Vehicle Fatal Crash Facts: 2022 Fatal/Fatality data

EXTERNAL: This email originated from outside of the State of Maine Mail System. Do not click links or open attachments unless you recognize the sender and know the content is safe.
Good morning Ted,

Hope you are well this morning.

It sounds to me like it could have been far worse! No seatbelt worn – ejected, no seatbelt worn – ejected, no seatbelts worn – all occupants ejected – driver fatality,…could have been worse!

I'm not a complete, cold and heartless bastard, as some might say, but why do I really have no sympathy here? In this day and age, no seatbelt worn, ejected? Not sure what more we, as highways safety professionals can do with this, over and above establishing primary laws, vigorously enforcing those laws, constant messaging and all that we are already doing.

A few things come to my mind here: You can lead a horse to water but you can't make it drink, and you can't fix stupid. Sucks to be you, rest in peace… stupid.

Sorry, I'm getting cynical in my old age!

Be smart, buckle up and have a great day folks!

Jeff

NH OFFICE OF HIGHWAY SAFETY
#GetHomeSafely
#CrashNotAccident

Jeffrey A. Landi
Law Enforcement Liaison/State Contracts
New Hampshire Department of Safety
33 Hazen Drive Room 208
Concord, NH 03305
Office: 603-271-2131
Direct: 603-271-6709
Email: jeffrey.landi@dos.nh.gov

Highway Safety Media Toolbox: https://www.trafficsafetymarketing.gov/

This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by law. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited and may be subject to criminal prosecution. If you have received this e-mail in error, please immediately notify me by telephone at (603) 271-2131.

From: Ted Minall <tedbb@aol.com>
Sent: Tuesday, June 14, 2022 7:50 PM
To: thomas.j.reagan@maine.gov; michael.sonia@pol.state.ma.us; Landi, Jeffrey <jeffrey.landi@dos.nh.gov>; Ruggiero, Paul <paul.ruggiero@dos.nh.gov>; Beauchamp, Roger <roger.beauchamp@dos.nh.gov>; richard.sullivan@risp.gov; bill.jenkins@partner.vermont.gov; paul.white@vermont.gov
Subject: Fwd: [Dps.alldre] Motor Vehicle Fatal Crash Facts: 2022 Fatal/Fatality data

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

OK, so continuing on our recent discussion, relating to fatalities in the 5 R-1 States, here's the very latest update from VT. There's no good news here. So, this is another "topic for discussion" for our long awaited face to face meeting in Concord, NH in August. If you have any questions, or suggestions, please let me know.

Thank you all, good night.

Ted

Ted Minall,
Law Enforcement Liaison
New England Traffic Safety, LLC
(802) 585-9531
On assignment to NHTSA

Sent from AOL Desktop

From: Mandy.White@vermont.gov
To: Mandy.White@vermont.gov
Sent: 6/14/2022 4:32:37 PM Eastern Standard Time
Subject: [Dps.alldre] Motor Vehicle Fatal Crash Facts: 2022 Fatal/Fatality data

--Fatal Crashes June 7, 2022 – June 13, 2022:

- 4/26/22: Shelburne, Falls Rd. Single vehicle ran off road. Driver fatality. Seatbelt worn.

- 6/6/22: Swanton, VT 78. Three vehicle crash involving a motorcycle, a box truck and a dump truck. Motorcyclist fatality. Unknown helmet use.

- 6/7/22: Bennington, US 7. Two vehicle crash with rollover. No seatbelts worn in Vehicle 1, all occupants ejected, driver fatality.

- 6/12/22: Grafton, Townshend Rd. Single vehicle ran off road into tree. Driver fatality. No seatbelt worn; ejected.

- 6/12/22: Chester, Davidson Hill Rd. Single vehicle ran off road into tree. Driver fatality. No seatbelt worn; ejected.

--**2022** Fatalities: **34** Total – **27** vehicle operators, **4** passengers, **3** pedestrians, **0** bicyclists

As of **June 13 in each calendar year shown**:

Year	Fatalities (People)	Fatal Crashes
2022	34	31
2021	24	21
2020	15	15
2019	8	8
2018	22	20

Fatal Crash Data	2022*	2021*	2020	2019	2018	2017
Total Fatal Crashes	31	69	58	44	61	64
Total Fatalities (People)	34	74	62	47	69	70
Double Fatality Crashes	3	5	4	3	8	3
Triple Fatality Crashes	0	0	0	0	0	0
Quadruple Fatality Crashes	0	0	0	0	0	1
Operators Suspected as Driving under the Influence of Alcohol Only	2	10	11	5	5	6
Operators Suspected as Driving under the Influence of Drugs Only	1	18	14	15	13	18
Operators Suspected as Driving under the Influence of both Alcohol & Drugs	6	12	6	2	10	11
Active Cannabis - Delta 9 THC Confirmed**	1	20	12	13	14	16
Operators Suspected of Speeding	2	32	15	14	22	27
Operators with Suspended License/ No License	1	7	13	5	7	11
Junior License Operators involved in fatal crashes	1	3	2	1	4	2
"Older Drivers" involved in fatal Crashes (Older Driver is defined as any person age 65 or older. & "involved" does not imply "fault")	12	19	15	16	14	15
Crashes involving a Large Truck/Bus ("involving" does not imply "fault")	6	4	3	10	7	5
Motorcyclist Fatalities	4	16	10	8	7	13

2021 data is as of the date of this report. These numbers are subject to change.

***Active Cannabis - Delta-9 THC Confirmed is counted in the number of operators that had drugs only or alcohol & drugs.*

Fatalities by Vehicle Type and Restraint/Safety Equipment Used							
Road User Type	**Restraint/Safety Equipment**	**2022**	**2021**	**2020**	**2019**	**2018**	**2017**
Motor Vehicle Occupant	Unbelted	18	28	24	17	34	24
	- Driver	14	25	19	15	25	17
	- Passenger	4	3	5	2	9	6
	- UTV Driver					0	1
	Belted	9	18	17	18	21	22
	- Driver	9	13	12	14	15	15
	- Passenger		5	5	4	6	7
	Improper Belt Use/Child Restraint			0	0	0	1
Motorcyclist/ATV	Wearing Helmet	3	13	10	5	5	11
	Non-DOT Compliant Helmet/Improper		2	0	1	1	1
	No Helmet		2	2	2	1	2
Vulnerable Users	Pedestrians	3	8	8	3	6	9
	Bicyclists			1	0	0	0
Unknown	Unknown Belt/Helmet Use	1	3	0	1	1	1
% Unbelted*		66%	61%	58%	49%	62%	52%
Total Fatalities		**34**	**74**	**62**	**47**	**69**	**70**

*Of all fatalities: only occupants in vehicles equiped with seatbelts are used in the calculation for unbelted percentage. Excludes: motorcycles, ATVs, pedestrians, bicyclists and unknowns. (Sum of Belted" & "Unbelted", divided into "Unbelted")

Mandy White | AOT Manager II & VT FARS Analyst
VTrans – Operations & Safety Bureau – Data Section
Dill Bldg. 2178 Airport Rd. Berlin, VT 05641
Cell Phone: [redacted]

Crash Help Line: (888)374-3011
Crash Email: AOT.CrashRequests@vermont.gov

DPS.AllDRE mailing list
DPS.AllDRE@list.vermont.gov
https://list.vermont.gov/mailman/listinfo/dps.alldre

From: Pack, Noah (POL)
To: Connolly, Kevin
Subject: RE: LPR Tenant MOU
Date: Wednesday, March 23, 2022 10:08:00 AM
Attachments: TRF-11 Nov21.pdf
image002.png

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: Connolly, Kevin <connollyk@barnstablepolice.com>
Sent: Wednesday, March 23, 2022 9:55 AM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Subject: RE: LPR Tenant MOU

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 can you please send me the most recent copy of your policy as well.

Thank you

Kevin A. Connolly
Detective Sergeant
Barnstable Police Department
Digital Forensics & Investigations Unit
USSS New England Cyber Fraud Task Force
508-958-6522
connollyk@barnstablepolice.com

From: Pack, Noah (POL) [mailto:noah.pack@state.ma.us]
Sent: Wednesday, March 23, 2022 9:50 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: LPR Tenant MOU

Hi Kevin,

Attached is the MOU that we discussed.

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

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From: Bryant, Michael
To: Pack, Noah (POL)
Subject: RE: LPR Tenant MOU
Date: Thursday, March 24, 2022 12:57:08 PM
Attachments: Yarmouth Policy Automatic License Plate Recognition.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.

Noah, I am working on the I.P. answer for you. I have attached our policy for your review to see if this will work or if we need to make any adjustments to it.

Thanks

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Cell 508-[redacted]
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Thursday, March 24, 2022 9:29 AM
To: Bryant, Michael <MBryant@yarmouth.ma.us>
Subject: LPR Tenant MOU

Attention!: This email originates outside of the organization. Do not open attachments or click links unless you are sure this email is from a known sender and you know the content is safe. Call the sender to verify if unsure. Otherwise delete this email.

Lieutenant Bryant,

Please see the attached tenant MOU and MSP policy. Thank you for your understanding and assistance.

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: Hession, Paul (POL)
To: Camoscio, Michael A.
Cc: Rob Law; Roy, Andrew M.; 4017164
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)
Date: Thursday, June 30, 2022 4:21:00 PM
Attachments: 280000_002 Security System Package_STV_MSP.pdf
MSP Sample Camera IP Schema 5218 v2.xlsx

Mike,

I provided some comments to the submittal. I also included this sample document if we can share with Signet with the submittal return so that we can prepare for what will be needed for the IP scheme and any needed network information from out IT folks.

Thanks
Paul

From: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>
Sent: Wednesday, June 29, 2022 7:14 PM
To: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Cc: Rob Law <rlaw@faainc.com>; Roy, Andrew M. <Andrew.Roy@stvinc.com>; 4017164 <4017164@stvinc.com>
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

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.

Paul,

We reviewed the Signet security submittal, overall it is very good. Do you want to have anyone at MSP take a look before we return?

Thank you,

Mike Camoscio
(p) 617-303-1135
(m) 857-[redacted]

From: Rob Simon (Daniel O'Connell's Sons Inc) <Daniel_O'Connell's_Sons@us02.procoretech.com>
Sent: Friday, June 24, 2022 12:51 PM
To: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>

Subject: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

****This e-mail is from outside STV****

MA State Police Barracks PCS

More details: View online | View PDF

DO NOT REPLY TO THIS EMAIL

This is a notification sent from an unmonitored email address.

Please click on the "View Online" link in this Email to reply to this Submittal in Procore.

Ryan Kane requires action from you on this submittal.

Project:	**MA State Police Barracks PCS**
Spec Section:	**280000 - Electronic Safety and Security (Trade Bid)**
Submittal #:	**280000-002.0**
Title:	**Security System - Head End Equipment Package**
Type:	**Shop Drawing**
Responsible Contractor:	**Jupiter Electric, Inc.**
Received From:	**Jordyn Goodwin**
Ball In Court:	**Mike Camoscio** **Paul Hession** **Rob Law** **Liam McHale** **Jenifer Olson** **Andrew Roy**
Submitter:	**Kane, Ryan (Daniel O'Connell's Sons Inc)** **Simon, Rob (Daniel O'Connell's Sons Inc)**
Approvers:	**Camoscio, Mike (STV, Inc.)** **Hession, Paul (Massachusetts State Police)**

	Law, Rob (Finegold Alexander Architects) **McHale, Liam (STV, Inc.)** **Olson, Jenifer (STV, Inc.)** **Roy, Andrew (STV, Inc.)**
Distribution:	**D'Alelio, John (Division of Capital Asset Management & Maintenance)** **Kane, Ryan (Daniel O'Connell's Sons Inc)** **McIntyre, Maureen (Division of Capital Asset Management & Maintenance)** **Walsh, Catherine (Division of Capital Asset Management & Maintenance)**
Due Date:	**07/08/22**
General Information Attachments:	**Submittal #21 Security System - Head End Equipment.pdf**
Submitter:	**Kane, Ryan (Daniel O'Connell's Sons Inc)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**
Submitter:	**Simon, Rob (Daniel O'Connell's Sons Inc)**
Date:	**Sent:** **Returned: 06/24/22**
Response:	**Submitted**
Attachments:	**Submittal 280000 Security System Package.pdf (Current)**
Comments:	**See attached submittal for Security System-Head End Equipment Package.**
Approver:	**Camoscio, Mike (STV, Inc.)**
Date:	**Sent:** **Returned:**

Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Hession, Paul (Massachusetts State Police)**
Date:	**Sent: 06/24/22** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Law, Rob (Finegold Alexander Architects)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**McHale, Liam (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Olson, Jenifer (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**

Attachments:	**None**
Comments:	**None**

Approver:	**Roy, Andrew (STV, Inc.)**
Date:	**Sent: 06/24/22** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

More details: View online | View PDF

Powered By Procore | support@procore.com | https://support.procore.com

Please consider the environment before printing this e-mail.

Redesigned and rebuilt: visit our new website at www.stvinc.com

The information contained in this electronic message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are informed that any dissemination, copying or disclosure of the material contained herein, in whole or in part, is strictly prohibited. If you have received this transmission in error, please notify STV and purge this message.

From: Camoscio, Michael A.
To: Hession, Paul (POL)
Cc: Rob Law; Roy, Andrew M.; 4017164
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)
Date: Wednesday, June 29, 2022 7:16:25 PM
Attachments: 280000_002 Security System Package_STV.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.

Paul,

We reviewed the Signet security submittal, overall it is very good. Do you want to have anyone at MSP take a look before we return?

Thank you,

Mike Camoscio
(p) 617-303-1135
(m) [redacted]

From: Rob Simon (Daniel O'Connell's Sons Inc) <Daniel_O'Connell's_Sons@us02.procoretech.com>
Sent: Friday, June 24, 2022 12:51 PM
To: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>
Subject: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

This e-mail is from outside STV

MA State Police Barracks PCS

More details: View online View PDF

DO NOT REPLY TO THIS EMAIL

This is a notification sent from an unmonitored email address.
Please click on the "View Online" link in this Email to reply to this Submittal in Procore.

Ryan Kane requires action from you on this submittal.

Project:	**MA State Police Barracks PCS**
Spec Section:	**280000 - Electronic Safety and Security (Trade Bid)**

Submittal #:	**280000-002.0**
Title:	**Security System - Head End Equipment Package**
Type:	**Shop Drawing**
Responsible Contractor:	**Jupiter Electric, Inc.**
Received From:	**Jordyn Goodwin**
Ball In Court:	**Mike Camoscio** **Paul Hession** **Rob Law** **Liam McHale** **Jenifer Olson** **Andrew Roy**
Submitter:	**Kane, Ryan (Daniel O'Connell's Sons Inc)** **Simon, Rob (Daniel O'Connell's Sons Inc)**
Approvers:	**Camoscio, Mike (STV, Inc.)** **Hession, Paul (Massachusetts State Police)** **Law, Rob (Finegold Alexander Architects)** **McHale, Liam (STV, Inc.)** **Olson, Jenifer (STV, Inc.)** **Roy, Andrew (STV, Inc.)**
Distribution:	**D'Alelio, John (Division of Capital Asset Management & Maintenance)** **Kane, Ryan (Daniel O'Connell's Sons Inc)** **McIntyre, Maureen (Division of Capital Asset Management & Maintenance)** **Walsh, Catherine (Division of Capital Asset Management & Maintenance)**
Due Date:	**07/08/22**
General Information Attachments:	**Submittal #21 Security System - Head End Equipment.pdf**
Submitter:	**Kane, Ryan (Daniel O'Connell's Sons Inc)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Submitter:	**Simon, Rob (Daniel O'Connell's Sons Inc)**
Date:	**Sent:** **Returned: 06/24/22**
Response:	**Submitted**
Attachments:	**Submittal 280000 Security System Package.pdf (Current)**
Comments:	**See attached submittal for Security System-Head End Equipment Package.**
Approver:	**Camoscio, Mike (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**
Approver:	**Hession, Paul (Massachusetts State Police)**
Date:	**Sent: 06/24/22** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**
Approver:	**Law, Rob (Finegold Alexander Architects)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**
Approver:	**McHale, Liam (STV, Inc.)**
Date:	**Sent:** **Returned:**

Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Olson, Jenifer (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Roy, Andrew (STV, Inc.)**
Date:	**Sent: 06/24/22** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

More details: View online | View PDF

Powered By Procore | support@procore.com | https://support.procore.com

Please consider the environment before printing this e-mail.

Redesigned and rebuilt: visit our new website at www.stvinc.com

The information contained in this electronic message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged,

confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are informed that any dissemination, copying or disclosure of the material contained herein, in whole or in part, is strictly prohibited. If you have received this transmission in error, please notify STV and purge this message.

From: Camoscio, Michael A.
To: Rob Law; Hession, Paul (POL)
Cc: Roy, Andrew M.; 4017164
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)
Date: Friday, July 1, 2022 1:28:14 PM
Attachments: image001.png
MSP Sample Camera IP Schema 5218 v2.xlsx
280000_002 Security System Package_STV_MSP_2022-07-01.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.

Rob,

Please return the attached update and the excel file as Revise and Resubmit.

They need to review the public desk location to confirm they are using a location already on the 30 kVa UPS.

Mike Camoscio
(p) 617-303-1135
(m) 857-[redacted]

From: Rob Law <rlaw@faainc.com>
Sent: Friday, July 1, 2022 1:09 PM
To: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>; paul.hession@state.ma.us
Cc: Roy, Andrew M. <Andrew.Roy@stvinc.com>; 4017164 <4017164@stvinc.com>
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

This e-mail is from outside STV

Hi all,

I know there is still some back and fourth needed, please let me know when all comments are complete and this is ready to go back, thanks!
Rob

Robert J. Law, AIA, NCARB
Senior Associate | Project Manager

FINEGOLD ALEXANDER ARCHITECTS
Office: 617.227.9272 x312

From: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>
Sent: Thursday, June 30, 2022 9:37 PM
To: paul.hession@state.ma.us
Cc: Rob Law <rlaw@faainc.com>; Roy, Andrew M. <andrew.roy@stvinc.com>; 4017164 <4017164@stvinc.com>

Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

Thanks Paul,

To your question on the [redacted]

[redacted]

Mike Camoscio
(p) 617-303-1135
(m) [redacted]

From: Hession, Paul (POL) <paul.hession@state.ma.us>
Sent: Thursday, June 30, 2022 4:22 PM
To: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>
Cc: Rob Law <rlaw@faainc.com>; Roy, Andrew M. <Andrew.Roy@stvinc.com>; 4017164 <4017164@stvinc.com>
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

****This e-mail is from outside STV****

Mike,

I provided some comments to the submittal. I also included this sample document if we can share with Signet with the submittal return so that we can prepare for what will be needed for the IP scheme and any needed network information from out IT folks.

Thanks
Paul

From: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>
Sent: Wednesday, June 29, 2022 7:14 PM
To: Hession, Paul (POL) <Paul.Hession@pol.state.ma.us>
Cc: Rob Law <rlaw@faainc.com>; Roy, Andrew M. <Andrew.Roy@stvinc.com>; 4017164 <4017164@stvinc.com>
Subject: RE: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

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.

Paul,

We reviewed the Signet security submittal, overall it is very good. Do you want to have anyone at MSP take a look before we return?

Thank you,

Mike Camoscio
(p) 617-303-1135
(m) [redacted]

From: Rob Simon (Daniel O'Connell's Sons Inc) <Daniel_O'Connell's_Sons@us02.procoretech.com>
Sent: Friday, June 24, 2022 12:51 PM
To: Camoscio, Michael A. <Michael.Camoscio@stvinc.com>
Subject: MA State Police Barracks PCS: Action Required for Submittal (#280000-002.0: Security System - Head End Equipment Package)

****This e-mail is from outside STV****

MA State Police Barracks PCS

[redacted]

More details: View online | View PDF

DO NOT REPLY TO THIS EMAIL

This is a notification sent from an unmonitored email address.

Please click on the "View Online" link in this Email to reply to this Submittal in Procore.

Ryan Kane requires action from you on this submittal.

Project:	**MA State Police Barracks PCS**
Spec Section:	**280000 - Electronic Safety and Security (Trade Bid)**
Submittal #:	**280000-002.0**
Title:	**Security System - Head End Equipment Package**
Type:	**Shop Drawing**
Responsible Contractor:	**Jupiter Electric, Inc.**
Received From:	**Jordyn Goodwin**
Ball In Court:	**Mike Camoscio** **Paul Hession** **Rob Law** **Liam McHale** **Jenifer Olson** **Andrew Roy**
Submitter:	**Kane, Ryan (Daniel O'Connell's Sons Inc)** **Simon, Rob (Daniel O'Connell's Sons Inc)**
Approvers:	**Camoscio, Mike (STV, Inc.)** **Hession, Paul (Massachusetts State Police)** **Law, Rob (Finegold Alexander Architects)** **McHale, Liam (STV, Inc.)** **Olson, Jenifer (STV, Inc.)** **Roy, Andrew (STV, Inc.)**
Distribution:	**D'Alelio, John (Division of Capital Asset Management & Maintenance)** **Kane, Ryan (Daniel O'Connell's Sons Inc)** **McIntyre, Maureen (Division of Capital Asset Management & Maintenance)**

	Walsh, Catherine (Division of Capital Asset Management & Maintenance)
Due Date:	**07/08/22**
General Information Attachments:	**Submittal #21 Security System - Head End Equipment.pdf**
Submitter:	**Kane, Ryan (Daniel O'Connell's Sons Inc)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**
Submitter:	**Simon, Rob (Daniel O'Connell's Sons Inc)**
Date:	**Sent:** **Returned: 06/24/22**
Response:	**Submitted**
Attachments:	**Submittal 280000 Security System Package.pdf (Current)**
Comments:	**See attached submittal for Security System-Head End Equipment Package.**
Approver:	**Camoscio, Mike (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**
Approver:	**Hession, Paul (Massachusetts State Police)**
Date:	**Sent: 06/24/22** **Returned:**

Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Law, Rob (Finegold Alexander Architects)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**McHale, Liam (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Olson, Jenifer (STV, Inc.)**
Date:	**Sent:** **Returned:**
Response:	**Pending**
Attachments:	**None**
Comments:	**None**

Approver:	**Roy, Andrew (STV, Inc.)**
Date:	**Sent: 06/24/22** **Returned:**
Response:	**Pending**
Attachments:	**None**

Comments: **None**

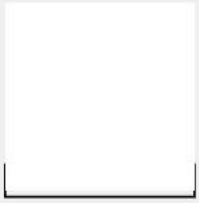
More details: View online | View PDF

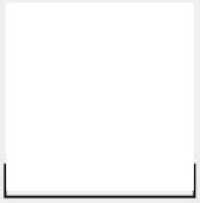
Powered By Procore | support@procore.com | https://support.procore.com

Please consider the environment before printing this e-mail.

Redesigned and rebuilt: visit our new website at www.stvinc.com









, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are informed that any dissemination, copying or disclosure of the material contained herein, in whole or in part, is strictly prohibited. If you have received this transmission in error, please notify STV and purge this message.

To:	Pack, Noah (POL)
Cc:	Silva, Kyra (POL); Biagi, Pamela (POL); Miller, Dianne (POL); Rossi, Gina (POL)
Subject:	RE: massDOT question
Date:	Thursday, January 20, 2022 10:18:50 AM
Attachments:	image001.png SCF_MSP_BainCor_executed.pdf massDOT_telecom_RFR.pdf Award - Bain Cor AW.pdf

Good morning Sgt. Pack,

The MSP-BainCor Inc. contract has been signed by both parties and is fully executed. I will send Mr. Bainter a copy for his file.

Looping in Pamela Biagi, Director of Fiscal Services.

Pam: this is a "piggyback" contract through MassDOT for a purchase of ALPR solar trailers. Also attached is the MassDOT contract for information purposes.

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:27 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. We hope to be purchasing solar trailers from Baincor.

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:25 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>

Subject: RE: massDOT question

Hi SGT Pack,

I will send out the SCF to Wayne Bainter at BainCor, Inc. I will cc you.

I apologize, can you refresh my memory? What is MSP purchasing from Baincor?

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:15 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. I will let our contact at Baincor know. Is there anything I can do to facilitate that contract execution?

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:13 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: FW: massDOT question

Hi Sgt. Pack,

Good news. As I mentioned, I hadn't heard back from John Polcari over at MassDOT, but a contact I have over there got back to me almost immediately. Please see below. MSP has been approved to utilize the MassDOT contract with Baincor under sperate contract execution. MassDOT is going to

send me a copy of the contract packet for our procurement file.

The last step will be for MSP to have an authorized signatory form Baincor sign a Standard Contract Form (SCF) and send it back to me for CAO Small's signature. I will have an SCF sent to the contract person at Baincor and keep you posted.

Thank you,
Brian

From: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday, January 18, 2022 1:48 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE: massDOT question

Hi Brian,

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it's open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet, which will include the executed SCF. Once I receive it, I will pass it along to you.

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 1:38 PM
To: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John,

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn't heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police
470 Worcester Road

Framingham, MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us



From: Kearnan, Brian J. (POL)
To: Pack, Noah (POL)
Cc: Silva, Kyra (POL); Biagi, Pamela (POL); Miller, Dianne (POL); Rossi, Gina (POL)
Subject: RE: massDOT question
Date: Thursday, January 20, 2022 10:19:14 AM
Attachments: image001.png
SCF_MSP_BainCor_executed.pdf
massDOT_telecom_RFR.pdf
Award - Bain Cor AW.pdf

Good morning Sgt. Pack,

The MSP-BainCor Inc. contract has been signed by both parties and is fully executed. I will send Mr. Bainter a copy for his file.

Looping in Pamela Biagi, Director of Fiscal Services.

Pam: this is a "piggyback" contract through MassDOT for a purchase of ALPR solar trailers. Also attached is the MassDOT contract for information purposes.

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:27 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. We hope to be purchasing solar trailers from Baincor.

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:25 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>

Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: RE: massDOT question

Hi SGT Pack,

I will send out the SCF to Wayne Bainter at BainCor, Inc. I will cc you.

I apologize, can you refresh my memory? What is MSP purchasing from Baincor?

Thank you,
Brian

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:15 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: Re: massDOT question

Thank you, Brian. I will let our contact at Baincor know. Is there anything I can do to facilitate that contract execution?

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: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 2:13 PM
To: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Subject: FW: massDOT question

Hi Sgt. Pack,

Good news. As I mentioned, I hadn't heard back from John Polcari over at MassDOT, but a contact I have over there got back to me almost immediately. Please see below. MSP has been approved to

utilize the MassDOT contract with Baincor under sperate contract execution. MassDOT is going to send me a copy of the contract packet for our procurement file.

The last step will be for MSP to have an authorized signatory form Baincor sign a Standard Contract Form (SCF) and send it back to me for CAO Small's signature. I will have an SCF sent to the contract person at Baincor and keep you posted.

Thank you,
Brian

From: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Sent: Tuesday, January 18, 2022 1:48 PM
To: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Subject: RE: massDOT question

Hi Brian,

Happy New Year to you as well! Good to hear from you.

I have reviewed the RFR and I concur that it's open for use for POL under separate contract execution; request to use approved. I have contacted our contracts and records department and requested the contract packet, which will include the executed SCF. Once I receive it, I will pass it along to you.

From: Kearnan, Brian J. (POL) <Brian.J.Kearnan@pol.state.ma.us>
Sent: Tuesday, January 18, 2022 1:38 PM
To: Bianchi, John D. (DOT) <John.D.Bianchi@dot.state.ma.us>
Subject: massDOT question

Hi John,

Happy New Year! I hope all is well.

The MSP is looking to piggyback off a massDOT Telecommunications RFR/contract. We saw that Mr. Polcari was a point of contact on COMMBUYS. I emailed on Thursday and hadn't heard. Please see the attached embedded thread. This is a bit of a rush on our end. Is there any way you could check on this for me or point me in the right direction?

Thanks John.

Brian

Brian J. Kearnan
Director of Contract Services
Massachusetts State Police

470 Worcester Road
Framingham, MA 01702
508-820-2127
Brian.J.Kearnan@pol.state.ma.us

From: Fecteau, Robert
To: Lorenco, Nicholas (POL); Pack, Noah (POL)
Cc: Kory Koster; Turner, Glenn; Gillham, Nicholas
Subject: ALPR Project- Commercial Vehicle Enforcement Section
Date: Monday, March 14, 2022 5:07:53 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.

Good Afternoon Gentlemen:
Trying hard not to overstep too far, I wanted to reach out via a group email and see if the two of you could provide some guidance on several technical details related to the ALPR project for the Commercial Vehicle Enforcement Section.

The challenges of physical installation notwithstanding, we feel that the success and efficiency of the project will hinge heavily on the coordination and control of the project's IT-related details: many/most of which are outlined below.

When each of you has a minute, can you please let us know who at MSP will have responsibility for the following:

1. Confirming that each vehicle has "an MDT" that meets or exceeds the following requirements:
   - Intel i3 CPU at 2.0 GHz (or Higher)
   - Windows Operating System (Windows 7 - Windows 10)
   - Microsoft .NET Framework v3.5
   - 8GM of RAM
   - 1GB of Free Disk Space
   - SVGA Display w/Minimum Resolution of 800 X 600 Pixels
   - Available 10/100 Ethernet Port (Dedicated to Neology, Static IP)
   - Keyboard, Mouse or Touchscreen Monitor
   - Internet Access (for Mapping & Firmware Updates)

2. Confirming that each vehicle has an MDT with a built-in "air card"
3. Confirming that each MDT has an available wired NIC port that we can use to connect the MDT to the vehicle's new ALPR processor
4. Confirming that we will be given rights/privileges on the MDT that will allow us to change the IP address and subnet mask of the wired NIC port to allow/support communication between the MDT and the ALPR processor (this is how camera data is received)
5. Confirming that we will be given rights/privileges on the MDT that will allow us to make any Windows settings changes required to ensure that the MDT's "air card' has priority over the computer's NIC (the "air card" is responsible for all other communication and for communication between PAGIS and BOSS)
6. Confirming that the "air card" in each vehicle will allow/support internet access and allow TCP/IP communication over Port [redacted] (this is the port/protocol over which PAGIS communicates to BOSS)
7. Confirming that we will be given rights/privileges on the MDT that will allow us to load Neology's PAGIS Software to the MDT
8. Confirming that MSP does not run any anti-virus or security suites that will impede the operation of PAGIS
9. Confirming that we will be given administrator access to the PAGIS Software to allow/support the

setup and configuration of the vehicle's ALPR cameras

I believe that Sgt. Pack has already taken care of #7, above, but it isn't clear who will be coordinating the remaining details.

Any assistance/guidance that you can provide would be greatly appreciated.

Thanks,
Bob

From: WSS Integrated Technologies
To: Commonwealth Fusion Center (POL)
Subject: Automatic License Plate Recognition (ALPR) For State and Municipal Applications – Free Webinar
Date: Friday, January 14, 2022 11:47:19 AM



Automatic License Plate Recognition (ALPR) is becoming an increasingly valuable tool for law enforcement agencies.

The ability to investigate, track, monitor and analyze data in real time has never been faster or easier. WSS Integrated Technologies is hosting a free webinar to demonstrate how ALPR can bring value to your state or municipality.

Here is what we will cover:

- **License plate verifications** - Verify license plate reads against hotlists and permit lists of vehicle plates to help you locate vehicles of interest and manage access to your parking space.
- **Suspicious vehicle pattern detection** - Trigger alarms and workflows when cameras repeatedly detect a vehicle of interest in an area according to pre-set thresholds.
- **Vehicle speed estimates** - Estimate the speed of vehicles to trigger alerts and reports to better detect road usage violations.
- **Vehicle classification and count** - Count and classify vehicles on the road by type for a better view of traffic volumes hourly, daily, monthly, and

annually.

- **Travel time reports** - Gather data needed to generate travel time reports based on an origin-destination matrix calculation.
- **Use Cases** – Demonstrate how other law enforcement agencies are using this technology to decrease cost and increases safety.

Register now to attend our free seminar on Tuesday, February 15th at 2:00pm EST by visiting our website under the COMPANY tab. Click the link below to go to directly to the registration form

Sign Up Now

If you can't make this webinar but would like to see a personal demo please reach out to us directly at info@wss-int.com or call us at 844-856-8071.



Copyright © 2022 WSS Integrated Technologies, All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
WSS Integrated Technologies
1052 Milford Warren Glen Rd
Bloomsbury, NJ 08804-2023

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: WSS
To: Commonwealth Fusion Center (POL)
Subject: Automatic license plate recognition for public sector applications
Date: Thursday, February 10, 2022 9:00:43 AM



Automatic License Plate Recognition (ALPR) is becoming an increasingly valuable tool for law enforcement agencies.

The ability to investigate, track, monitor and analyze data in real time has never been faster or easier. WSS Integrated Technologies is hosting a free webinar to demonstrate how ALPR can bring value to your state or municipality.

Here is what we will cover:

- **License plate verifications** - Verify license plate reads against hotlists and permit lists of vehicle plates to help you locate vehicles of interest and manage access to your parking space.
- **Suspicious vehicle pattern detection** - Trigger alarms and workflows when cameras repeatedly detect a vehicle of interest in an area according to pre-set thresholds.
- **Vehicle speed estimates** - Estimate the speed of vehicles to trigger alerts and reports to better detect road usage violations.
- **Vehicle classification and count** - Count and classify vehicles on the road by type for a better view of traffic volumes hourly, daily, monthly, and

annually.

- **Travel time reports** - Gather data needed to generate travel time reports based on an origin-destination matrix calculation.
- **Use Cases** – Demonstrate how other law enforcement agencies are using this technology to decrease cost and increases safety.

Register now to attend our free seminar on Tuesday, February 15th at 2:00pm EST by visiting our website under the COMPANY tab. Click the link below to go to directly to the registration form

Sign Up Now

If you can't make this webinar but would like to see a personal demo please reach out to us directly at info@wss-int.com or call us at 844-856-8071.



Copyright © 2022 WSS Integrated Technologies, All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
WSS Integrated Technologies
1052 Milford Warren Glen Rd
Bloomsbury, NJ 08804-2023

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: McCarthy, Steven (POL)
Subject: Bill may classify some gun owners as LE; Clemency floated for 19 cops
Date: Thursday, February 24, 2022 4:13:29 PM

February 24, 2022 | View as webpage | Too many emails? Update Subscription Preferences

TOP STORIES

Chicago cops must abide by COVID vaccine mandate, arbitrator rules

The vaccine rule led the city and the Fraternal Order of Police to sue each other

Texas deputy fatally shot while working off-duty security at mall

'The Old West': Tenn. bill would classify some gun owners as 'law enforcement'

Suspect who shot Fla. deputy is killed by homeowner during break-in

Texas governor suggests clemency for 19 indicted Austin cops

Goat helps make arrest by chasing suspect, Va. cops say

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

CASE REVIEW

Eighth Circuit rejects qualified immunity for police supervisory and subordinate officers in crowd control operation

By Mike Callahan

Jury trial required to determine liability for mass arrest, alleged excessive force and supervisory indifference

Decision not to conduct DNA testing didn't defeat conviction

By Ken Wallentine

Does failure to collect DNA evidence change the outcome of a recent case or will eyewitness accounts be sufficient?

State and NIBRS Reporting, Done Right!

CivicEye delivers cloud-based software solutions to public safety and law enforcement professionals that

enhance daily workflows and improve community outcomes. Designed by public safety professionals to make a difference.

Schedule a demo today

FOOT PURSUITS



Don't let your guard down during a foot pursuit

By Gordon Graham

Suspects can easily ambush an officer on foot



7 stages of a successful foot pursuit

By Lt. Dan Marcou

To win these encounters, it is good to look at these real world-obstacle courses as a seven-stage event



SPONSORED CONTENT



Putting family at the heart of mental health

The Axon Aid: Wellness program aims to bridge the communication gap between law enforcement personnel and their loved ones.

FEATURED RESOURCES

Download the Police1 Training Simulator Buying Guide
Get the guide

FEATURED JOB

Police Officer - $25,000 Lateral Incentive and $10,000 Entry Level Incentive
$6,001 - $8,041 per month/Officer- 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 © 2022 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: P1 Product Bulletin
To: McCarthy, Steven (POL)
Subject: Check Out the Latest Police Products
Date: Thursday, December 22, 2022 12:16:46 PM

December 22, 2022 | View as webpage

Direct communication to all of your candidates, instantly

Message all candidates with a personalized touch using bulk text-message communication. Import existing candidates and have conversations at scale.

Book Demo

Avon Protection C50

The Avon C50 APR is based on the U.S. M50/JSGPM (Joint Services General Purpose Mask), provides maximum operational flexibility to counter multiple threats including CBRN agents, TICs, and TIMs, outstanding field of vision, and superior comfort.

Experience the C50 APR

Connecticut's rapid DNA program helps close cases faster

With 24/7 access to Rapid DNA technology to generate real-time investigative leads Connecticut's rapid DNA program has been an overwhelming success opening new possibilities to quickly solve and prevent crimes.

Learn more

Increase your de-escalation options with this powerful hand-held restraint device

Currently, officers must move from verbal commands to pain compliance. With the BolaWrap, they can move from verbal commands to restraint, and end an encounter without using higher levels of force.

Learn more

New ALPR system puts dent in Ohio city's crime



What could police do with not just still images but high-quality video and advanced AI analysis of vehicles passing key points in their city? In Bowling Green they're using it to solve a wide range of cases even beyond the traffic realm.



Find out how 

Fully Loaded Patrol RIBs Deliverable within 30-days



Our boats are available on GSA Advantage with eligibility to purchase under the 1122 program.



See Our Models 



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 © 2022 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: WSS
To: Commonwealth Fusion Center (POL)
Subject: Free Webinar for Automatic License Plate Recognition Solutions
Date: Tuesday, January 25, 2022 11:45:03 AM



Automatic License Plate Recognition (ALPR) is becoming an increasingly valuable tool for law enforcement agencies.

The ability to investigate, track, monitor and analyze data in real time has never been faster or easier. WSS Integrated Technologies is hosting a free webinar to demonstrate how ALPR can bring value to your state or municipality.

Here is what we will cover:

- **License plate verifications** - Verify license plate reads against hotlists and permit lists of vehicle plates to help you locate vehicles of interest and manage access to your parking space.
- **Suspicious vehicle pattern detection** - Trigger alarms and workflows when cameras repeatedly detect a vehicle of interest in an area according to pre-set thresholds.
- **Vehicle speed estimates** - Estimate the speed of vehicles to trigger alerts and reports to better detect road usage violations.
- **Vehicle classification and count** - Count and classify vehicles on the road by type for a better view of traffic volumes hourly, daily, monthly, and

annually.

- **Travel time reports** - Gather data needed to generate travel time reports based on an origin-destination matrix calculation.
- **Use Cases** – Demonstrate how other law enforcement agencies are using this technology to decrease cost and increases safety.

Register now to attend our free seminar on Tuesday, February 15th at 2:00pm EST by visiting our website under the COMPANY tab. Click the link below to go to directly to the registration form

Sign Up Now

If you can't make this webinar but would like to see a personal demo please reach out to us directly at info@wss-int.com or call us at 844-856-8071.



Copyright © 2022 WSS Integrated Technologies, All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
WSS Integrated Technologies
1052 Milford Warren Glen Rd
Bloomsbury, NJ 08804-2023

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: Driscoll, Francis (POL)
To: Robles, Francis Jr. (POL); Kelleher, John (POL); Moran, Mathew (POL)
Subject: Fw: Motorola meeting
Date: Wednesday, February 23, 2022 9:49:04 AM

You are more than welcome to join the meeting. I don't know if we have a room yet but I will let you know.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 22, 2022 at 6:43:16 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**
>
> 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.
> Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if that would be ok. Thanks again.
>
> Jim
>
> On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us>

wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
> Major Matthew Murphy
> Det. Captain Steve McCarthy
> Lieutenant Francis Driscoll
> Sergeant Noah Pack
> Sergeant Nicholas Nason
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, thanks Captain. I'll just await a date that works best for you.
> >
> > Jim
> >
> > On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
> >
> > > Sure Jim.
> > >
> > > Detective Captain Steven McCarthy
> > > Massachusetts State Police
> > > Division of Homeland Security and Preparedness
> > > 470 Worcester Rd
> > > Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 470 Worcester Road
> Framingham, MA 01702
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling

<jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL)
<steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager

Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Pack, Noah (POL)
To: Egnitz, Brian (POL)
Subject: Fwd: ALPR Project- Commercial Vehicle Enforcement Section
Date: Monday, March 14, 2022 5:16:57 PM

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: Fecteau, Robert <fecteaur@bcmcontrols.com>
Sent: Monday, March 14, 2022 4:26:07 PM
To: Lorenco, Nicholas (POL) <nicholas.lorenco@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Cc: Kory Koster <kkoster@329marketinginc.com>; Turner, Glenn <Turnerg@bcmcontrols.com>; Gillham, Nicholas <gillhamn@bcmcontrols.com>
Subject: ALPR Project- Commercial Vehicle Enforcement Section

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 Gentlemen:
Trying hard not to overstep too far, I wanted to reach out via a group email and see if the two of you could provide some guidance on several technical details related to the ALPR project for the Commercial Vehicle Enforcement Section.

The challenges of physical installation notwithstanding, we feel that the success and efficiency of the project will hinge heavily on the coordination and control of the project's IT-related details: many/most of which are outlined below.

When each of you has a minute, can you please let us know who at MSP will have responsibility for the following:

1. Confirming that each vehicle has "an MDT" that meets or exceeds the following requirements:
   - Intel i3 CPU at 2.0 GHz (or Higher)
   - Windows Operating System (Windows 7 - Windows 10)
   - Microsoft .NET Framework v3.5
   - 8GM of RAM
   - 1GB of Free Disk Space
   - SVGA Display w/Minimum Resolution of 800 X 600 Pixels
   - Available 10/100 Ethernet Port (Dedicated to Neology, Static IP)
   - Keyboard, Mouse or Touchscreen Monitor
   - Internet Access (for Mapping & Firmware Updates)

2. Confirming that each vehicle has an MDT with a built-in "air card"
3. Confirming that each MDT has an available wired NIC port that we can use to connect the MDT to the

vehicle's new ALPR processor

4. Confirming that we will be given rights/privileges on the MDT that will allow us to change the IP address and subnet mask of the wired NIC port to allow/support communication between the MDT and the ALPR processor (this is how camera data is received)
5. Confirming that we will be given rights/privileges on the MDT that will allow us to make any Windows settings changes required to ensure that the MDT's "air card' has priority over the computer's NIC (the "air card" is responsible for all other communication and for communication between PAGIS and BOSS)
6. Confirming that the "air card" in each vehicle will allow/support internet access and allow TCP/IP communication over Port [redacted] (this is the port/protocol over which PAGIS communicates to BOSS)
7. Confirming that we will be given rights/privileges on the MDT that will allow us to load Neology's PAGIS Software to the MDT
8. Confirming that MSP does not run any anti-virus or security suites that will impede the operation of PAGIS
9. Confirming that we will be given administrator access to the PAGIS Software to allow/support the setup and configuration of the vehicle's ALPR cameras

I believe that Sgt. Pack has already taken care of #7, above, but it isn't clear who will be coordinating the remaining details.

Any assistance/guidance that you can provide would be greatly appreciated.

Thanks,
Bob

From: steven.mccarthy@pol.state.ma.us
To: Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); Driscoll, Francis (POL); Egnitz, Brian (POL)
Cc: Connor, Debora (POL)
Subject: Fwd: Follow Up
Date: Wednesday, February 16, 2022 2:56:48 PM

Good day sirs,

Please see below message from Motorola and let me know your availability for a meeting during the week of 2/28.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 15, 2022 at 8:39:50 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**
>
> 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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.
>
> Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team
>
> Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC

State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim
>
> On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'll check with the rest of the team and get back to you soon.
> >
> > The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow

that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.

Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.

I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From:	McCarthy, Steven (POL)
To:	Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); Driscoll, Francis (POL); Egnitz, Brian (POL)
Cc:	Connor, Debora (POL)
Subject:	Fwd: Follow Up
Date:	Wednesday, February 16, 2022 2:56:49 PM

Good day sirs,

Please see below message from Motorola and let me know your availability for a meeting during the week of 2/28.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 15, 2022 at 8:39:50 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC

State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim
>
> On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'll check with the rest of the team and get back to you soon.
> >
> > The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow

that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.

Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.

I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

From: steven.mccarthy@pol state.ma.us
To: JAMES DOWLING
Cc: Driscoll Francis (POL)
Subject: Fwd: Motorola meeting
Date: Wednesday, February 23, 2022 2:59:49 PM

Hi Jim,

If you send me the team email addresses we will forward a calendar invite.

Thanks
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state ma.us>
> **Date:** February 23, 2022 at 1:13:12 PM EST
> **To:** "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
> **Subject: Re: Motorola meeting**
>
> No problem. Can you send me the email for the Motorola reps. I'll send an invite out with projected location.
>
> ---
>
> **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Sent:** Wednesday, February 23, 2022 11:54 AM
> **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> **Subject:** Re: Motorola meeting
>
> Great thanks Frank
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:
> >
> > Sir,
> >
> > I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.
> >
> > ---
> >
> > **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> > **Sent:** Wednesday, February 23, 2022 10:41 AM
> > **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> > **Subject:** Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if

that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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.
>
> Steve, when you have a chance, could you provide the titles of the MSP

attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:
>
> > Should have it soon.
> >
> > Detective Captain Steven McCarthy

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best

of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion

some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his

replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: McCarthy, Steven (POL)
To: JAMES DOWLING
Cc: Driscoll, Francis (POL)
Subject: Fwd: Motorola meeting
Date: Wednesday, February 23, 2022 2:59:50 PM

Hi Jim,

If you send me the team email addresses we will forward a calendar invite.

Thanks
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state ma.us>
> **Date:** February 23, 2022 at 1:13:12 PM EST
> **To:** "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
> **Subject: Re: Motorola meeting**
>
> No problem. Can you send me the email for the Motorola reps. I'll send an invite out with projected location.
>
> ---
>
> **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Sent:** Wednesday, February 23, 2022 11:54 AM
> **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> **Subject:** Re: Motorola meeting
>
> Great thanks Frank
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:
> >
> > Sir,
> >
> > I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.
> >
> > ---
> >
> > **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> > **Sent:** Wednesday, February 23, 2022 10:41 AM
> > **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> > **Subject:** Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if

that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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.
>
> Steve, when you have a chance, could you provide the titles of the MSP

attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:
>
> > Should have it soon.
> >
> > Detective Captain Steven McCarthy

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best

of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion

some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his

replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: John Dobberstein, Managing Editor, SecurityInfoWatch.com
To: Crouse, David (POL)
Subject: Integrator Newswire: Vanguard Awards: Retrofitting security upgrades in 100+ buildings
Date: Tuesday, November 22, 2022 3:48:09 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.

SIW Integrator Newswire ENL | View online

securityinfowatch.com header logo

November 22, 2022

FEATURED STORY

Massive Upgrade in Harris County, Texas

By John Dobberstein

Vanguard Award Honorable Mention: Multi-

year retrofit project involved security technology upgrades in more than 150 buildings in the downtown Houston area

SIW November 30th Webinar: 4 Biometric Access Control Trends You Can't Ignore in 2023

Date: November 30, 2022 Time: 1:00 PM EST / 12:00 PM CST / 10:00 AM PST / 6:00 PM GMT Sponsor(s): Alcatraz AI Duration: 1 HourRegister Today! Already registered? Please click here to log in!A certificate of attendance will be offered.The access control industry can be filled with so many new and emerging innovations that can be hard to keep up with...

TOP NEWS

Genetec AutoVu ALPR cameras enabling new services, efficiencies for car wash franchises

By collecting and correlating data from AutoVu LPR cameras, Sonny's The CarWash Factory is able to further increase the value of their POS solution to car wash operators.

NSCA sponsoring fundraiser to help support workforce development

Join 'Be the Spark,' our virtual fundraiser to help Ignite attract and retain next-gen workers to the commercial integration industry

Oosto Chief AI scientist tells ISC East attendees about a bold new vision for video analytics

Dieter Joecker, Oosto's chief technology officer says "semantic segmentation enables contextual analytics to achieve a holistic understanding of video footage in real-time."

SEPTA board approves ZeroEyes gun detection pilot program

SEPTA is the first major transit system to deploy ZeroEyes' solution, which is used by the U.S. Department of Defense, public school districts and universities, Fortune 500 corporate campuses and many other organizations across more than 30 states.

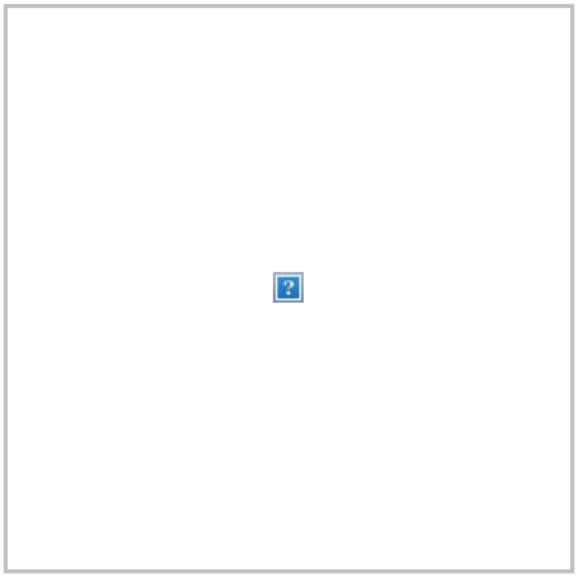
SecuriThings partners with Axis Communications physical security device management

The partnership improves customers' end-to-end visibility and control, helping ensure that their physical security devices run reliably and securely over their entire lifecycle.

MCP helps Massachusetts State Police upgrade radio system

The new system will improve coverage, capacity, reliability, and interoperability to enhance emergency communications for field responders, helping them perform better and more safely.

BEST OF SECURITY BUSINESS



The Smart Money: Three Hot Trends in Residential Security

By Jennifer Kent

From inflation to product innovation and MDU expansion, residential integrators have a lot to pay attention to in the fourth quarter

PRODUCT WATCH



Invixium IXM VERTU card and mobile access reader

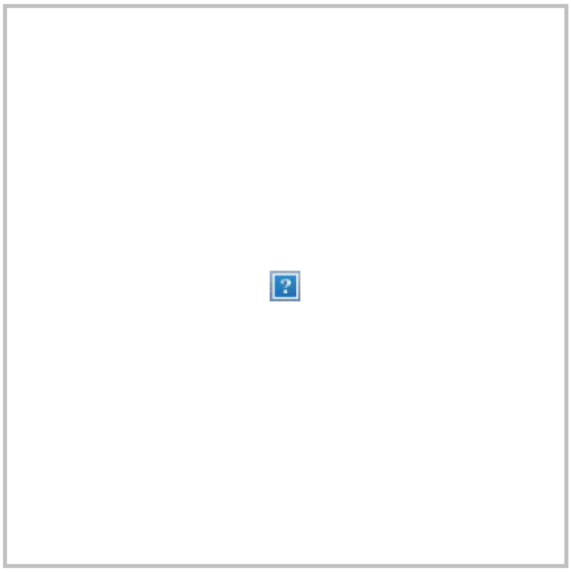


Cynalytica SerialGuard ICS Cybersecurity Solution



Arcules Forensic Video Search

MEDIA CENTER



GSX 2022 Show Floor Spotlight: Milestone Systems, Inc.

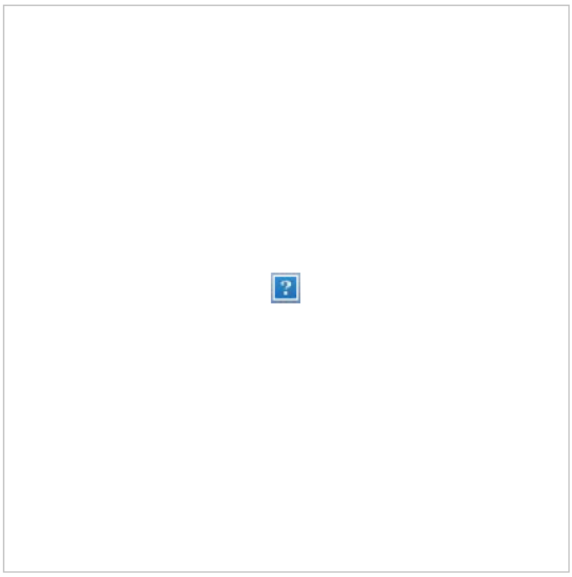
How data-driven video technology can empower an organization's risk posture

Read More



Vintra Guard module AI-assisted access control

EVENT WATCH



CAA Winter Convention

11/30/2022 7:00 AM CST - 12/03/2022 9:00 AM CST
https://www.caaonline.org/winter-convention/

Now in it's 30th year, the CAA Winter Convention & Annual Fundraiser has evolved into the premier event in California serving the Electronic Security Industry. This year's event will be held at the Fairmont Hotel in San Francisco from Nov. 30-Dec. 3, where we once again aim to inspire and educate generations of industry leadership by providing upda...

Home | Contact Us | Subscribe | Advertise

© 2022 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
30 Burton Hills Blvd., Suite 185
Nashville, TN 37215

From: Warren, Rosemary (POL)
To: Egnitz, Brian (POL); Nason, Nicholas (POL); zzSojka, Robert (POL); Quinn, Dermot (POL); Tucker, Daniel T (POL); Murphy, Matthew G - DIS (POL); Wilcox, Christopher (POL); Driscoll, Francis (POL); McCarthy, Steven (POL); zzRange, Scott (POL); Cyr, Mark (POL); Pack, Noah (POL)
Date: Thursday, May 19, 2022 8:48:31 AM

Brian - Kelly asked if we still were "holding" on the ALPR purchases?

From: Jussaume, Carolyn B
To: Sullivan, Margaret (POL)
Cc: Michalski, Maria (EPS)
Subject: MDT Image & Security Questions - MSP Cruiser project
Date: Thursday, January 6, 2022 3:03:21 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.

Peg

As we finalize our approach for the MSP cruiser as a mobile office project, we request some time on EOPSS calendars to discuss our approach and clarify a few areas around security, MDT imaging, and support. Below are a few of the areas that we would like to discuss with you and the team.

Thank you for your help- it is much appreciated

Carolyn

MDT Image

Current process: Could you explain how this process is handled today and what from you would like to see changed in this process?

Image- MSP would like us to image the MDT as part of the service. Would the Commonwealth provide us (or a partner such as panasonic) the image for the MDT? Or would you still want to image the MDTs and we would collect and install? What is included in the image? Will we need to provide antivirus/antimalware etc? Would ZIA be included?

Application Updates: We understand that the Commonwealth is using intune today provision/patch the MDTs.(is that correct?) If we are imaging the MDT, what would be the best process for EOTSS and Verizon to send any updates for state applications to the MDTs?

Applications being accessed: Our understanding is the following:

CJIS- accessed through a web browser

Other applications accessed- email (O365,), RAMS,ASIS, other state applications for time reporting etc These applications are accessed through centrify VPN session. Are we missing anything?

Identity creation & provisioning-

How are personnel onboarded and offboarded? We thought that the Commonwealth could create the identity and we would provision the MDT based on the policies defined by the Commonwealth- is that reasonable?

MDT Disposal & handling-

Just wanted to confirm the requirements before an MDT is sent for service- we are assuming the device is wiped by EOTSS/EOPSS today before it is sent for repair. At the end of the service term, Verizon would own the asset. Would there be any additional requirements beyond wiping the device?

Help Desk- if we are trouble shooting an issue and it appears to be a state application issue, what should be the process to engage and work with the Commonwealth help desk?

Security: Zero trust architecture

We were thinking about using ZScaler Private Access, building on the ZIA that the Commonwealth has already deployed. From our perspective it would offer the following benefits:

Increased visibility: This would provide Verizon and the Commonwealth with better application performance visibility for troubleshooting purposes to minimize trouble resolution time.

Cloud migration- As the Commonwealth migrates various applications to the cloud such as ALPR, this minimize user impact. Zscaler Private Access works the same in AWS, Azure and GCP as it does in a physical data center so any migration of Apps to the cloud would be seamless.

Build on existing investment- deployed on the user end through the Z App that the Commonwealth has installed.

We would like to understand the Commonwealth's ' perspective on this approach.

Implementation

If we were were to include ZScaler Private Access, we would need to plan the implementation for the pilot.

(***information from ZScaler below***)

We understand that required effort for new projects is a concern and wanted to provide some detail so that all parties can understand that the POV for enhanced secure cruiser testing can be up and running in as little as 2 hours in a working session. We would want to have a 1-hour planning session to understand and detail requirements, timing and gather a few other details. Very quickly after that, Zscaler could have the ZPA cloud instance provisioned and ready.

The Zscaler solution requires no hardware and for POV purposes we need just 1 to 2 virtual machines deployed in the State's data center environment. Beyond that an integration with Azure AD would be needed for authentication. All of this work is guided by an experienced Zscaler technical resource.

From the Cruiser perspective, Zscaler's ZIA service is currently running there on an already installed Zscaler client (Zscaler Client Connector) on the machine. We would simply activate the new (ZPA) service and at the next daily login any enrolled user would be able to use Zscaler to access private data center applications.

Lastly, the test POV tenant would convert to the State Police's permanent tenant. All work done for the POV will be preserved and used to quickly enable the entire user population

--



Carolyn Jussaume

Business Development
Massachusetts Government Team

Verizon Business Group

M 617 699 3900
100 Causeway Street
Boston, Massachusetts 02114



From: Dr. Lou Marciani
To: Carmichael, James (POL)
Subject: MEDIA RELEASE: IIFX Celebrates Key Additions to FANCENTRIC & Expo Conference Lineup
Date: Wednesday, May 4, 2022 10:31:02 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.

Image

MEDIA RELEASE: FOR IMMEDIATE RELEASE

Media Contact: Ben Whiteside bwhiteside@focusgroupms.com ([redacted] (cell)

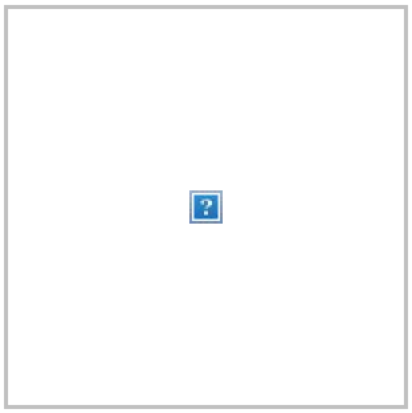
FANCENTRIC Master Color.png

IIFX Celebrates Key Additions to FANCENTRIC Conference & Expo Lineup

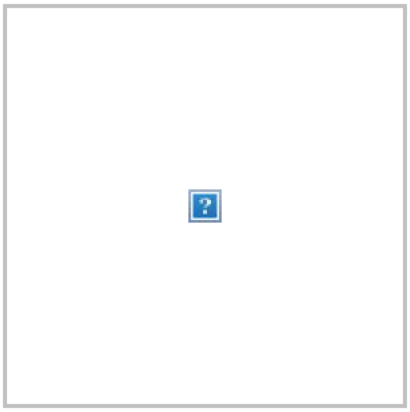
For images and logo for this release, visit this link: https://www.dropbox.com/sh/kovd0c6qazwbo4m/AADKqWDq_ik3Id25VOt6BG9Na?dl=0

May 3, 2022 Jackson, Mississippi – From Tuesday, May 24 to Thursday, May 26, the **Innovation Institute for Fan Experience (IIFX)** will host its first in-person **FANCENTRIC™** International Conference & Expo at **Caesars Palace** in Las Vegas, Nevada. The Conference & Expo will bring together leading thought leaders, subject matter experts and vendors from all aspects of the sports and entertainment industry. Leading up to the Conference & Expo, IIFX will be highlighting speakers and their experience in the industry. This week, IIFX would like to showcase some key additions to the conference agenda.

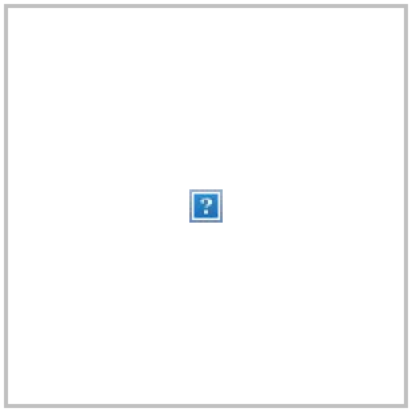
Register for the FANCENTRIC Conference & Expo



Matt Kenny serves Executive Vice President of Operations and Events for the Kansas City Chiefs. In his fifth year with the Club he is responsible for the fan experience at GEHA Field at Arrowhead Stadium, including parking and logistics, event operations, guest services, and the club's relationships with concessions and merchandise partners.He also oversees Arrowhead Events, the non-football revenue-generating arm of the Chiefs, the team's training camp and is the club's main point of contact with theJackson County Sports Complex Authority. Additionally, the security, stadium operations and facilities functions for Arrowhead Stadium and The University of Kansas Health System Training Complex report to him.Kenny serves as the executive committee for the KC 2026 World Cup bid, and as a board member of the Kansas City Sports Commission and the Stadium Managers Association.

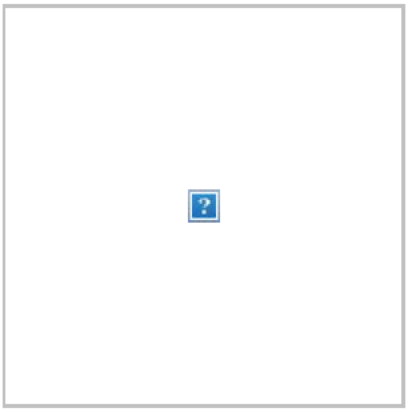


Dr. Lindsay Gietzen is a University professor and program director where she specializes in simulation and educational evaluation. As a physician's assistant, she practiced in emergency/trauma medicine in Detroit, Michigan and then specialized in neurological surgery, leading a team that developed and performed many procedures for the first time in the United States. She is a Member of the Michigan Academy of Physician Assistants, American Academy of Physician Assistants, Physician Assistant Education Association, and Director at Large of the Association of Neurosurgical Physician Assistants. Lindsay is currently serving an appointment to the American Council onEducation, where she is an expert faculty evaluator for military medical programs on behalf of the Department of Defense.

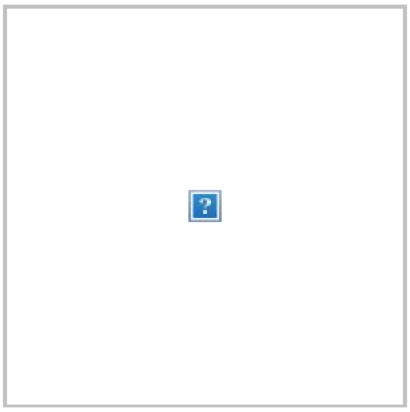


Ryan McConnell is the lead product manager for Kantar's North American MONITOR suite of syndicated consumer insights products. His role is to lead the strategy, content, and innovation plans for MONITOR's business, which has been helping brand marketers understand the attitudes, values, and motivations of American consumers for 50+ years. Ryan began his career in marketing and advertising as a media planner at Ogilvy & Mather in 1999. After a stint as a consumer strategist at Carat, Ryan earned

his master's degree in journalism at NYU and worked as a reporter for MLB.com and Advertising Age prior to joining The Futures-Company – which later became Kantar – in 2008. In March 2020, Ryan's passion for sports marketing led him to spearhead the creation of Sports MONITOR, a fan insights service that helps brands connect with modern fans.



Chris Yigit is the Technology Partnership Manager for AutoVu™, the automatic license plate recognition (ALPR) solution from Genetec™, overseeing strategic technology partnerships, integrations and alliances. Chris joined the company in April 2010 and has been instrumental ingrowing the AutoVu product line ever since.Chris began his career as an applications engineer at Loctite Canada and then at Matrox VideoProducts where he held various managerial positions spanning over 10 years. Chris holds aBachelor of Engineering from McGill University in Quebec, Canada.



Philippe Bourdarias has 20 years' experience in the sport industry and the organization of major sport events. He started his sport career in Spain where he contributed to the development of Beach Soccer, first for "Octagon", an international sport agency, and then for "FIFA Beach Soccer".Philippe then joined World Rugby where he spearheaded the global event strategy and organization of over 100events including 7 Rugby World Cups (Men, Women's, and Rugby Sevens).He was also a driving force behind the development of Rugby Sevens which culminated with its inclusion in the Olympic Games inRio 2015. Philippe also worked with the UCI where he headed-up the Sport department. In 2019, he transitioned over to the world of Esports joining Zwift, an award-winning cycling and running virtual platform to lead their Esports Strategy, where he created the cycling esports discipline in partnership with the UCI. Philippe joined One Plan in 2021 to lead the development of the company in the sport and major event sector.

Purchase Single Day FANCENTRIC Ticket HERE

These industry leaders will join the diverse group of individuals who will be speaking at the FANCENTRIC Conference. The **speakers** highlighted today will be joining confirmed speakers **Larry Olmsted**, **Russ Simons**, **Lee Zeidman**, **Kim Stone**, **Mario Coutinho**, **Jim Mercurio**, **Paul Turner** , **Scott McCartney**, **John Petrone**, **Shawn Trell**, **Nick Spampanato**, **Pat Christenson**, **Julie Giese**, **Jeff Keas**, **Brian Herbert**, **Laura Edell**, **Eric Golebiewski**, **Daniel Heal**, **Dr. Todd**

Harple, **Lisa Furfine**, **Jennifer "Jae" Pi'ilani Requiro**, **Dan Donovan**, **Kasia Hanson**, **Matt Pasco**, **Dr. Tilman Jolly**, and many others.

Discounted rooms are available through the **IIFX FANCENTRIC** block through 5/6/2022. Rooms with competitive rates are available at all Caesars properties through **Caesars.com**.

Visit the official **FANCENTRIC** website to learn more about conference details, **sponsorship** and **exhibitor** opportunities. To register, you can purchase a ticket **HERE**.

##

About the Innovation Institute for Fan Experience

*Founded in 2020 in the midst of the pandemic by veteran industry leaders. IIFX's vision is to be the leading and most trusted global authority on providing exceptional fan experience for sports and entertainment. With offices in the USA, UK and Canada, IIFX produces content, events, and facilitates dialogue and collaboration in in the sports and entertainment industry around its core areas of expertise. Visit: **iifx.org** for more.*

About Dr. Lou Marciani: Read more at this link.

Follow us on the following social media:

Facebook CLICK HERE

Twitter CLICK HERE

LinkedIn CLICK HERE

Instagram CLICK HERE

YouTube CLICK HERE

If you would rather not receive future communications from The Innovation Institute for Fan Experience, let us know by clicking here.
The Innovation Institute for Fan Experience, 4780 I-55 N, Suite 100, Jackson, Mississippi 39211 United States

From: steven.mccarthy@pol.state.ma.us
To: Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); Driscoll, Francis (POL); Nason, Nicholas (POL); Pack, Noah (POL); Egnitz, Brian (POL); Connor, Debora (POL)
Cc: Warren, Rosemary (POL); JAMES DOWLING
Subject: Motorola meeting
Date: Wednesday, February 23, 2022 9:03:26 AM

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy

Lieutenant Francis Driscoll

Sergeant Noah Pack

Sergeant Nicholas Nason

Mr. Brian Egnitz

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,

Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.

Let me know,

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that

need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
>
> SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager

Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

From: McCarthy, Steven (POL)
To: Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); Driscoll, Francis (POL); Nason, Nicholas (POL); Pack, Noah (POL); Egnitz, Brian (POL); Connor, Debora (POL)
Cc: Warren, Rosemary (POL); JAMES DOWLING
Subject: Motorola meeting
Date: Wednesday, February 23, 2022 9:03:26 AM

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 22, 2022 at 6:43:16 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**
>
> 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.
>
> Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if that would be ok. Thanks again.
>
> Jim
>
> On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > Probable attendees:
> >
> > Lt. Colonel Christopher Wilcox
> >
> > Major Matthew Murphy
> >
> > Det. Captain Steve McCarthy

Lieutenant Francis Driscoll

Sergeant Noah Pack

Sergeant Nicholas Nason

Mr. Brian Egnitz

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,

Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.

Let me know,

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that

need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
>
> SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager

Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

From: Flock Safety Product Team
To: Egnitz, Brian (POL)
Subject: New Interactive Dispatch Map and live video are here!
Date: Wednesday, June 8, 2022 1:58:59 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.



JUNE 2022

NEWSLETTER

This monthly newsletter is here to keep you informed about all the latest product enhancements, success stories, and events at Flock Safety.

Island



Eliminate Crime. Build Community.

Did you know that Flock Safety works with over 45 K-12 school districts and universities nationwide to help prevent crime on campus? Traditional cameras don't have the ability to prevent offenders from entering campus with real-time alerts, gleaned from objective evidence such as license plates. Flock Safety also helps campuses gain actionable evidence to help solve crimes such as motor vehicle theft, drug trafficking, parking lot break-ins, and more. Interested in learning more? Check out this story on how Purdue University has partnered with Flock Safety and their local police department to reduce crime in the community.

If there's a school district or university that could benefit from proactive alerts, please reach out to us below — our school safety team will be in touch.

Get in Touch

Live video is here!

Did you know that Flock Safety offers the ability to connect third-party IP cameras from across jurisdictions (public or private) and display them alongside Hot List alerts, AVL data, traffic conditions, and more, **at no cost?**

When you combine actionable evidence from a Flock

ALPR with Livestream Video + VMS, you can:

- Access live on-scene video from your Dispatch Map and Live Video Gallery for better incident response and management
- Unlock enhanced situational awareness for more leads, faster incident response, and increased officer safety
- Build stronger cases with video replay, 7-day video retention, and MP4 downloads

Get Started with Flock Safety

Gondola



Island



Flock helps Locate Missing Woman in Northport

A 34-year-old woman went missing on Friday, June 3rd, and the only information the Local PD had of her last known location was driving from Northport to Alexander City. However, through the use of Flock Safety cameras, police located her safely. Learn more below.

Watch Now

Flock in the Field

Our Flock Safety team enjoys hosting and attending events so we can meet potential customers, like you! This month you can catch our team at:

- Tennessee School Resources Officers Annual Conference - 6/12
- Major County Sheriffs Association Summer Conference - 6/13
- GA FBINAA Summer Conference - 6/26
- National Sheriffs Association Conference - 6/27
- Police Security Expo - 6/28

We also are hosting a few Flock Events such as:

- White Hall User Group (Arkansas) - 6/8
- Trussville User Group (Alabama) - 6/15
- Educational Webinar: Organized Retail Crime (digital) - 6/28

If you have any questions or would like more information, get in touch below!

Gondola

Get in Touch

Flock Safety is officially serving the Commercial community, focusing on protecting businesses of all types and sizes. If you know of a company that could benefit from Flock, please send their contact information below.

Send Info

Logo

1170 Howell Mill Rd NW, Suite 210, Atlanta, Georgia 30318, United States

2021 © All rights reserved

Unsubscribe

From: Flock Safety Product Team
To: Mason, Christopher (POL)
Subject: New Interactive Dispatch Map and live video are here!
Date: Wednesday, June 8, 2022 3:11:30 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.

JUNE 2022

NEWSLETTER

This monthly newsletter is here to keep you informed about all the latest product enhancements, success stories, and events at Flock Safety.

Island

Eliminate Crime. Build Community.

Did you know that Flock Safety works with over 45 K-12 school districts and universities nationwide to help prevent crime on campus? Traditional cameras don't have the ability to prevent offenders from entering campus with real-time alerts, gleaned from objective evidence such as license plates. Flock Safety also helps campuses gain actionable evidence to help solve crimes such as motor vehicle theft, drug trafficking, parking lot break-ins, and more. Interested in learning more? Check out this story on how Purdue University has partnered with Flock Safety and their local police department to reduce crime in the community.

If there's a school district or university that could benefit from proactive alerts, please reach out to us below — our school safety team will be in touch.

Get in Touch

Live video is here!

Did you know that Flock Safety offers the ability to connect third-party IP cameras from across jurisdictions (public or private) and display them alongside Hot List alerts, AVL data, traffic conditions, and more, **at no cost?**

When you combine actionable evidence from a Flock

ALPR with Livestream Video + VMS, you can:

- Access live on-scene video from your Dispatch Map and Live Video Gallery for better incident response and management
- Unlock enhanced situational awareness for more leads, faster incident response, and increased officer safety
- Build stronger cases with video replay, 7-day video retention, and MP4 downloads

Get Started with Flock Safety

Gondola



Island



Flock helps Locate Missing Woman in Northport

A 34-year-old woman went missing on Friday, June 3rd, and the only information the Local PD had of her last known location was driving from Northport to Alexander City. However, through the use of Flock Safety cameras, police located her safely. Learn more below.

Watch Now

Flock in the Field

Our Flock Safety team enjoys hosting and attending events so we can meet potential customers, like you! This month you can catch our team at:

- Tennessee School Resources Officers Annual Conference - 6/12
- Major County Sheriffs Association Summer Conference - 6/13
- GA FBINAA Summer Conference - 6/26
- National Sheriffs Association Conference - 6/27
- Police Security Expo - 6/28

We also are hosting a few Flock Events such as:

- White Hall User Group (Arkansas) - 6/8
- Trussville User Group (Alabama) - 6/15
- Educational Webinar: Organized Retail Crime (digital) - 6/28

If you have any questions or would like more information, get in touch below!

Gondola

Get in Touch

Flock Safety is officially serving the Commercial community, focusing on protecting businesses of all types and sizes. If you know of a company that could benefit from Flock, please send their contact information below.

Send Info

Logo

1170 Howell Mill Rd NW, Suite 210, Atlanta, Georgia 30318, United States

2021 © All rights reserved

Unsubscribe

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: PD disables social media comments; S.F. reverses lethal police robot policy
Date: Wednesday, December 7, 2022 5:06:43 PM

December 7, 2022 | View as webpage | Too many emails? Update Subscription Preferences

Dear Police1 Member,

Understanding how case law guides department policies and procedures is critical for ensuring an officer makes not only the best decision but also the most legally defensible decision.

Join us for a webinar on Dec. 12 in which Chief Ken Wallentine and Terrence Dwyer will review:

- Evolving standards in use of force review
- Stop and frisk pitfalls
- Handling First Amendment audits
- Workplace conduct problems

RSVP here.

Stay safe,

— *The Police1 Team*

TOP STORIES

San Francisco supervisors bar police robots from using lethal force for now

The board sent the issue back for further discussion and could vote in the future to let police use robots in a lethal manner in limited cases

Ore. AG: Measure 114 won't go into effect after state judge's ruling

Md. PD disables social media comments due to 'divisive and hateful' climate

Report: Nearly 27% of LAPD's lowest-ranked officers are female

Ill. gov. signs amendment to criminal justice overhaul weeks before cash bail set to end

'We're talking a quarter-inch from tragedy': Calif. deputy survives after being shot in the head

10% Tuition discount for law enforcement and government employees.

Fully online self-paced degree programs.

Learn more about CCU

BOSS4 – Managed Service ALPR Solution

Intuitive searching and analytics, including powerful map-based, multi-location, searching capability. Our MANTIS 4-D Vehicle Recognition solution provides rich data mining capabilities to find the vehicles you are looking for.

Discover your options

FEATURED CONTENT

The pros and cons of the Invest to Protect Act

By Kathleen Dias

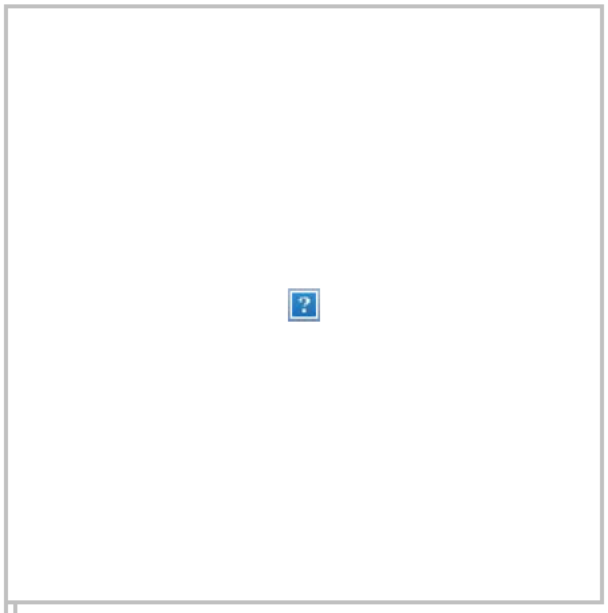
If signed into law, it would provide $60 million in grants each year to "smaller" law enforcement agencies, from 2023 to 2027

"Let's get it on!": The passing of a legend

By Tim Dees

There will never be another one like Mills Lane

Mobile computing for law enforcement





Put important data in your teams' hands with rugged tablets that can withstand the elements and work as long and hard as they do.

Sign up

IMPAIRED DRIVING PREVENTION MONTH



DWI investigations: Officers can avoid field sobriety tests missteps with practice

By Deputy James "Zack" Holley

Attention to timing, instructions and demonstrations help reveal intoxication clues during pre-arrest screening



How the art of conversational interrogation will improve your DWI investigations

By Val Van Brocklin

Most real-life police interviews contain many undesirable practices – here's how to improve them



SPONSORED CONTENT



A better way to slow speeders and protect workers in construction zones

A new approach to traffic monitoring and enforcement is more effective in slowing traffic over a longer distance in areas like construction zones.

FEATURED JOB

Police Officer - $25,000 Lateral Incentive and $10,000 Entry Level Incentive
$6,001 - $8,041 per month/Officer- Vancouver, Washington

FEATURED RESOURCES

How to Buy Radios (eBook)
Download this Police1 radios buying guide to learn key steps for product selection, purchasing and implementation.

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 © 2022 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Southeastern WI Threat Analysis Center
To: Stelmat, Jason (POL)
Subject: RE: Automated License Plate Recognition (ALPR) - response requested
Date: Thursday, February 3, 2022 1:52:29 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.

Jason,

Please see STAC's answers below.

> **From:** "Stelmat, Jason (POL)" <jason.stelmat@state.ma.us>
> **Date:** February 3, 2022 at 8:46:20 AM CST
> **Subject: Automated License Plate Recognition (ALPR) - response requested**
>
> Good morning folks,
> I am the privacy officer for the Commonwealth Fusion Center (Massachusetts). I have been asked to gather information regarding nationwide use of Automated License Plate Recognition (ALPR) systems. If you are able to respond, I am seeking the following:
>
> 1) Is the use of ALPR legal in your state?
>   a. Yes
>
> 2) If yes, do law enforcement agencies in your state use ALPR?
>   a. Yes
>
> 3) If yes, does your Fusion Center have access to ALPR data either internally or through another agency?
>   a. Yes
>
> 4) If yes, is there a centralized program for accessing ALPR data (i.e. do all requests within your state have to be submitted to a specific agency to obtain ALPR data or do agencies have independent access)?
>   a. No centralized processing
>
> 5) Are there specific requirements for accessing ALPR data (e.g. pending investigation, warrant, exigent circumstances, etc.)?
>   a. Yes, must be tied to an investigation; criminal predicate
>
> Any information you are able to provide is helpful and greatly appreciated. Please let me know if there is any questions or concerns you are experiencing related to the use of ALPR. If needed, my direct contact information is below but email is the best way to reach me.

Respectfully,
Jason

Jason R. Stelmat | **Privacy Officer**
Massachusetts State Police | Commonwealth Fusion Center
124 Acton Street, Maynard MA 01754
direct 978-451-3752 | fax 978-451-3767

Southeastern Wisconsin Threat Analysis Center
749 West State Street Milwaukee, WI 53233
Office: 414.935.7741
Fax: 414.935.7052
WiWatch.org



NOTICE: **This E-mail and any attachments may contain information that is law enforcement sensitive or for official use only. Use and further disclosure of the information by the recipient must be consistent with applicable laws, regulations and agreements. See, Wis. Stat. §§ 19.36(2) & (8); 18 U.S.C. § 2510-2520; 42 U.S.C. § 3782; & 28 CFR Part 23. If you received this E-mail in error, please notify the sender; delete the E-mail; and do not use, disclose or store the information it contains.**

The City of Milwaukee is subject to Wisconsin Statutes related to public records. Unless otherwise exempted from the public records law, senders and receivers of City of Milwaukee e-mail should presume that e-mail is subject to release upon request, and is subject to state records retention requirements. See City of Milwaukee full e-mail disclaimer at www.milwaukee.gov/email_disclaimer

From: Bryant, Michael
To: Pack, Noah (POL)
Subject: RE: Cape LPR Training
Date: Monday, June 27, 2022 3:03:14 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.

Noah for the training we will have:

Det. Lt. Mike Bryant	mbryant@yarmouth.ma.us
Sgt. Scott Lundegren	slundegren@yarmouth.ma.us
Det. Eric Nuss	enuss@yarmouth.ma.us
Det Chris Kent	ckent@yarmouth.ma.us
Det. Dave Schneeweis	dschneeweis@yarmouth.ma.us
Det. Jeff Rivett	jrivett@yarmouth.ma.us
Det. Connor Burnham	cburnham@yarmouth.ma.us

Unable to attend but will need access:

Det. Sgt. Steve Renzi	renzi@yarmouth.ma.us
Det. Mike Zontini	zontini@yarmouth.ma.us

Let me know if you need anything else…

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Cell 508[redacted]
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

From: Pack, Noah (POL) <noah.pack@state.ma.us>
Sent: Friday, June 17, 2022 4:45 PM
To: Bryant, Michael <MBryant@yarmouth.ma.us>; Lundegren, Scott <SLundegren@yarmouth.ma.us>; Connolly, Kevin <connollyk@barnstablepolice.com>; Cleve Daniels <cdaniels@town.dennis.ma.us>
Cc: Wilcox, Christopher (POL) <christopher.wilcox@state.ma.us>; Egnitz, Brian (POL)

<brian.egnitz@state.ma.us>
Subject: Cape LPR Training

> **Attention!:** This email originates outside of the organization. Do not open attachments or click links unless you are sure this email is from a known sender and you know the content is safe. Call the sender to verify if unsure. Otherwise delete this email.

Sirs:

The State Police's Automatic License Plate Recognition system has been updated and transitioned to new software. We will provide a training session on this new system for your agencies on **June 28, 2022, at 10:30 AM** at the **Barnstable Police Department.**

Training will include an update on the program, account setup/familiarization, and hands-on use of the new system with discussion of strategies, best practices, and privacy considerations. Attendees will benefit immensely by bringing a computer to use during the training to set up their accounts. This training is intended for a limited number of individuals selected by the Dennis, Yarmouth, and Barnstable police departments to have access to search and enter plates into this new system.

We have been working full-time on getting this project back online and updated into the modern era of policing. During the training, we will welcome your feedback on how the ALPR system has or has not worked and how it might best serve its public safety purpose for your communities. I look forward to meeting you all soon.

Respectfully,

Noah

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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Tuesday, February 22, 2022 4:38:03 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.

Thank you!

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

Hi Jim,

I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will

have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look

forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



For more information on how and why we collect your personal

information, please visit our Privacy Policy.

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: McCarthy, Steven (POL)
To: Jim Dowling
Subject: RE: Follow Up
Date: Wednesday, February 16, 2022 3:25:00 PM

Hi Jim,

I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim
>
> On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'll check with the rest of the team and get back to you soon.
> >
> > The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could

benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.

I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling

Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: McCarthy, Steven (POL)
To: JAMES DOWLING
Cc: Wilcox, Christopher (POL); Murphy, Matthew G - DIS (POL); Driscoll, Francis (POL); Pack, Noah (POL); Egnitz, Brian (POL); Connor, Debora (POL)
Subject: Re: Follow Up
Date: Tuesday, February 22, 2022 9:25:36 AM

Good morning Jim,

Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.

Let me know,

SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim
>
> On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'll check with the rest of the team and get back to you soon.
> >
> > The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a

cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola. I am sure his successor will be as well, and I look

forward to meeting them when they are available.

There are two things you can help me with.
The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,
SM

Detective Captain Steven McCarthy #1477
Executive Officer: Planning, Preparedness, and Response Section
Massachusetts State Police
Division of Homeland Security and Preparedness
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Monday, February 21, 2022 1:08:20 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.

Hi Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

I have no doubt Jim, thank you.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,

I'll check with the rest of the team and get back to you soon.

The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>

Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together

from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Driscoll, Francis (POL)
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Thursday, February 17, 2022 9:09:53 AM

Sir,

Also, I am available most days except Wednesday.

Thanks,

Frank

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 16, 2022 2:56 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Subject: Fwd: Follow Up

Good day sirs,

Please see below message from Motorola and let me know your availability for a meeting during the week of 2/28.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 15, 2022 at 8:39:50 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical

resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.
>
> Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, January 31, 2022 7:11 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Follow Up
>
> 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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Driscoll, Francis (POL)
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Thursday, February 17, 2022 9:08:17 AM

Sir,

I am available all day Monday.

Thanks,

Frank

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 16, 2022 2:56 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Subject: Fwd: Follow Up

Good day sirs,

Please see below message from Motorola and let me know your availability for a meeting during the week of 2/28.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 15, 2022 at 8:39:50 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical

resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.
>
> Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, January 31, 2022 7:11 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Follow Up
>
> 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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:50:50 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.

Thanks!

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052
> >
> > On Feb 16, 2022, at 9:08 PM, Jim Dowling

<jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,

I'll check with the rest of the team and get back to you soon.

The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard.

Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive

Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: McCarthy, Steven (POL)
To: JAMES DOWLING
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:28:46 PM

Should have it soon.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>> Sure Jim.
>>
>> Detective Captain Steven McCarthy
>> Massachusetts State Police
>> Division of Homeland Security and Preparedness
>> 470 Worcester Rd
>> Framingham, MA 01702
>> 508-867-1052
>>
>>> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>>>
>>> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at

the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email?

Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state

agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

From: steven.mccarthy@pol.state.ma.us
To: JAMES DOWLING
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:28:46 PM

Should have it soon.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052
> >
> > > On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> > >
> > > 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at

the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email?

Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state

agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:11:32 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.

Great, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: McCarthy, Steven (POL)
To: JAMES DOWLING
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:09:49 PM

Sure Jim.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>

Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front

plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to

provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: steven.mccarthy@pol.state.ma.us
To: JAMES DOWLING
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:09:47 PM

Sure Jim.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>

Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front

plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to

provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 9:08:08 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.

Captain, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>

Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

Hi Jim,

Sorry for the delay in responding.

Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.

I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805

E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 3:27:32 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.

Captain, thanks for the update.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

Hi Jim,

Sorry for the delay in responding.

Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.

I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805

E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Wilcox, Christopher (POL)
To: McCarthy, Steven (POL); Murphy, Matthew G - DIS (POL); Driscoll, Francis (POL); Egnitz, Brian (POL)
Cc: Connor, Debora (POL)
Subject: Re: Follow Up
Date: Wednesday, February 16, 2022 3:06:58 PM

Steve - Tuesday I am pretty much booked up

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

508 820-7301

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 16, 2022 2:56 PM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Subject: Fwd: Follow Up

Good day sirs,

Please see below message from Motorola and let me know your availability for a meeting during the week of 2/28.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 15, 2022 at 8:39:50 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, could you let me know your availability next week for a call or two

on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, January 31, 2022 7:11 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Follow Up
>
> 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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Subject: Re: Follow Up
Date: Tuesday, February 15, 2022 8:39:51 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.

Hi Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
>
> SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805

E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: McCarthy, Steven (POL)
To: Jim Dowling
Subject: RE: Follow Up
Date: Tuesday, February 22, 2022 3:41:00 PM

Hi Jim,

Probable attendees:

Lt. Colonel Christopher Wilcox
Major Matthew Murphy
Det. Captain Steve McCarthy
Lieutenant Francis Driscoll
Sergeant Noah Pack
Sergeant Nicholas Nason
Mr. Brian Egnitz

SM

Detective Captain Steven McCarthy #1477
Executive Officer: Planning, Preparedness, and Response Section
Massachusetts State Police
Division of Homeland Security and Preparedness
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,

Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.

Let me know,

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
> >
> > Jim
> >
> > On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
> >
> > > Hi Jim,

I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and

federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look

forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

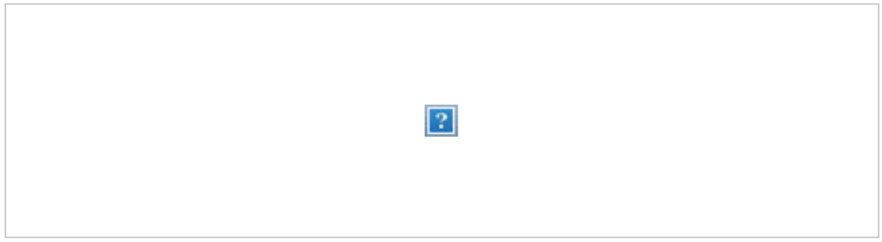


For more information on how and why we collect your personal information, please visit our Privacy Policy.

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: steven.mccarthy@pol.state.ma.us
To: JAMES DOWLING
Cc: Driscoll, Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 3:28:33 PM

Thanks Jim

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 3:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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.

Sure, here is the attendee list. Thank you!

sam rabadi@motorolasolutions.com
jdowling@motorolasolutions.com
kevin.johnson3@motorolasolutions.com
daniel.wilburn@motorolasolutions.com
alan melvin@motorolasolutions.com

Jim

On Wed, Feb 23, 2022 at 3:00 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> If you send me the team email addresses we will forward a calendar invite.
>
> Thanks
> Steve
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> Begin forwarded message:
>
> > **From:** "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state ma.us>
> > **Date:** February 23, 2022 at 1:13:12 PM EST
> > **To:** "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
> > **Subject: Re: Motorola meeting**
> >
> > No problem. Can you send me the email for the Motorola reps. I'll send an invite out with projected location.
> >
> > ---
> >
> > **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> > **Sent:** Wednesday, February 23, 2022 11:54 AM
> > **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> > **Subject:** Re: Motorola meeting

Great thanks Frank

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Sir,

I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 10:41 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police

Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)"
<steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL)
<steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL)
<steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL)
> <steven mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy
> >
> > Massachusetts State Police
> >
> > Division of Homeland Security and Preparedness
> >
> > 470 Worcester Rd
> >
> > Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State

Highway Patrol, Motorola
Public Safety Intelligence-Led
Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain
Steven McCarthy #1477

Executive Officer:
Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Warren, Rosemary (POL)
To: McCarthy, Steven (POL)
Subject: RE: Motorola meeting
Date: Wednesday, February 23, 2022 9:10:19 AM

Good Morning,

Just FYI, I do not have a Conference Room due to Trial Boards and the HSOC is closed due to monitor replacements.

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: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 22, 2022 at 6:43:16 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
> Major Matthew Murphy
> Det. Captain Steve McCarthy
> Lieutenant Francis Driscoll
> Sergeant Noah Pack
> Sergeant Nicholas Nason
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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.
>
> Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.
>
> Jmi
>
> On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL)

<steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Should have it soon.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052
> >
> > On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
> >
> > Jim
> >
> > On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
> >
> > > Hi Jim,
> > >
> > > I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
> > >
> > > SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling
<jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL)
<steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support

Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's

the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: Driscoll, Francis (POL)
To: Connor, Debora (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 1:09:35 PM

Yes & yes. I advised the DCap that Fleet would like to attend. So for the larger group I arranged we can use either the Watch Center conference table or if necessary the HSOC main room will be empty.

From: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 12:48 PM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Cc: Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Subject: RE: Motorola meeting

Frank – just checking in. Has anyone made arrangements for a conference room? If not, can you please do this and send out a calendar invite so everyone that should be in attendance is reminded.

Thanks much!

-Debora

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 22, 2022 at 6:43:16 PM EST

To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
> Major Matthew Murphy
> Det. Captain Steve McCarthy
> Lieutenant Francis Driscoll
> Sergeant Noah Pack
> Sergeant Nicholas Nason
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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.
>
> Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back

soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Should have it soon.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052
> >
> > On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
> >
> > SM

Detective Captain Steven McCarthy
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible,

presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,
SM

Detective Captain Steven McCarthy #1477
Executive Officer: Planning, Preparedness, and Response Section
Massachusetts State Police
Division of Homeland Security and Preparedness
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: McCarthy, Steven (POL)
To: Driscoll Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 11:54:29 AM

Great thanks Frank

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Sir,

I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 10:41 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:
>
> > Hi Jim,

I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on

the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM

Detective Captain Steven McCarthy
#1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting

them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: steven.mccarthy@pol.state.ma.us
To: Driscoll, Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 11:54:28 AM

Great thanks Frank

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Sir,

I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 10:41 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:
>
> > Hi Jim,

I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on

the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM

Detective Captain Steven McCarthy
#1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting

them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Driscoll Francis (POL)
To: McCarthy Steven (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 11:40:12 AM

Sir,

I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 10:41 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

> On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:
>
> Thank you. Fleet may send a representative or two.
>
> ---
>
> **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Sent:** Wednesday, February 23, 2022 9:03 AM
> **To:** Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
> **Cc:** Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
> **Subject:** Motorola meeting
>
> Good morning,
>
> Motorola good to go next Monday morning at GHQ.
>
> Respectfully,
> Steve
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702

508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
> Major Matthew Murphy
> Det. Captain Steve McCarthy
> Lieutenant Francis Driscoll
> Sergeant Noah Pack
> Sergeant Nicholas Nason
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:
>
> > Should have it soon.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052
> >
> > On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
> >
> > Jim
> >
> > On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:
> >
> > > Hi Jim,
> > >
> > > I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
> > >
> > > SM
> > >
> > > Detective Captain Steven McCarthy
> > > Division of Homeland Security and Preparedness

Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach.
> Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a

broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,
SM

Detective Captain Steven McCarthy #1477
Executive Officer: Planning, Preparedness, and Response Section
Massachusetts State Police
Division of Homeland Security and Preparedness
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling

Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: McCarthy_Steven (POL)
To: Driscoll_Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 10:41:37 AM

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>

Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led

Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a

broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

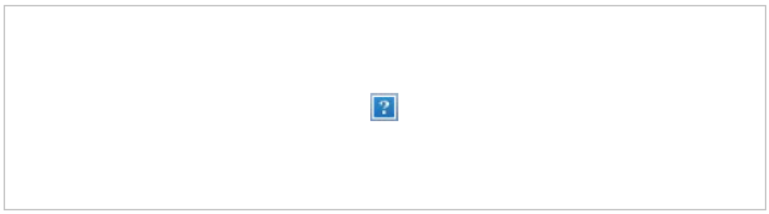


For more information on how and why we collect your personal information, please visit our Privacy Policy.

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



For more information on how and why we collect your personal information,

> > *please visit our Privacy Policy.*

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling

Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: steven.mccarthy@pol state.ma.us
To: Driscoll, Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 10:41:36 AM

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>

Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy

Massachusetts State Police

Division of Homeland Security and Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led

Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.
>
> Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a

broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

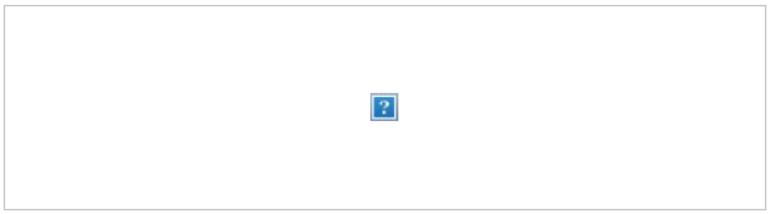


For more information on how and why we collect your personal information, please visit our Privacy Policy.

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



For more information on how and why we collect your personal information,

> > *please visit our Privacy Policy.*

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling

Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Driscoll, Francis (POL)
To: McCarthy, Steven (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 9:49:57 AM

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Date:** February 22, 2022 at 6:43:16 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Follow Up**
>
> 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.
>
> Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if that would be ok. Thanks again.
>
> Jim
>
> On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

Hi Jim,

Probable attendees:

Lt. Colonel Christopher Wilcox
Major Matthew Murphy
Det. Captain Steve McCarthy
Lieutenant Francis Driscoll
Sergeant Noah Pack
Sergeant Nicholas Nason
Mr. Brian Egnitz

SM

Detective Captain Steven McCarthy #1477
Executive Officer: Planning, Preparedness, and Response Section
Massachusetts State Police
Division of Homeland Security and Preparedness
508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 470 Worcester Road
> Framingham, MA 01702
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 15, 2022 8:39 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll

assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Division of Homeland Security and Preparedness
> Massachusetts State Police
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 6:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, could you let me know your availability next week for a call or two on the topics you

referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?
>
> Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.
>
> Thanks,
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, January 31, 2022 7:11 PM

To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.

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

From: McCarthy, Steven (POL)
To: Warren, Rosemary (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 9:11:44 AM

I think we can fit in our lunch room.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:10 AM, Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us> wrote:

Good Morning,

Just FYI, I do not have a Conference Room due to Trial Boards and the HSOC is closed due to monitor replacements.

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: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
> Major Matthew Murphy
> Det. Captain Steve McCarthy
> Lieutenant Francis Driscoll
> Sergeant Noah Pack
> Sergeant Nicholas Nason
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'm checking with our people and should have a

date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule

permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE

video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

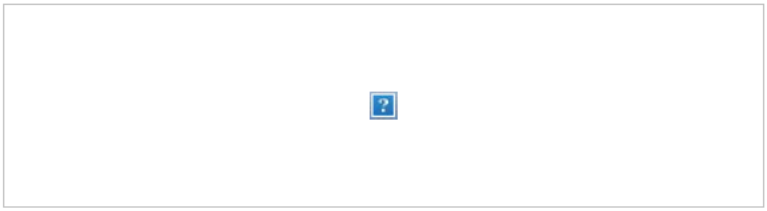
M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: steven.mccarthy@pol.state.ma.us
To: Warren, Rosemary (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 9:11:43 AM

I think we can fit in our lunch room.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:10 AM, Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us> wrote:

Good Morning,

Just FYI, I do not have a Conference Room due to Trial Boards and the HSOC is closed due to monitor replacements.

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: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
> Major Matthew Murphy
> Det. Captain Steve McCarthy
> Lieutenant Francis Driscoll
> Sergeant Noah Pack
> Sergeant Nicholas Nason
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
> Executive Officer: Planning, Preparedness, and Response Section
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, February 21, 2022 1:07 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > I'm checking with our people and should have a

date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.

SM

Detective Captain Steven McCarthy

Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule

permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE

video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

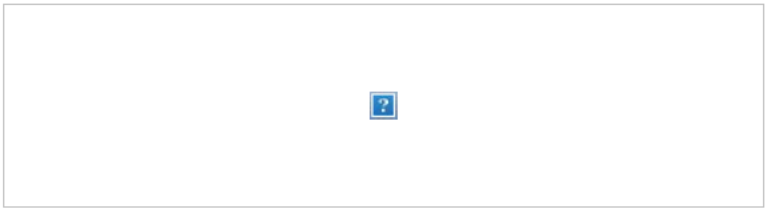
M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

From: McCarthy, Steven (POL)
To: JAMES DOWLING
Cc: Driscoll, Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 3:28:33 PM

Thanks Jim

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 3:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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.

Sure, here is the attendee list. Thank you!

sam rabadi@motorolasolutions.com
jdowling@motorolasolutions.com
kevin.johnson3@motorolasolutions.com
daniel.wilburn@motorolasolutions.com
alan melvin@motorolasolutions.com

Jim

On Wed, Feb 23, 2022 at 3:00 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> If you send me the team email addresses we will forward a calendar invite.
>
> Thanks
> Steve
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> Begin forwarded message:
>
> > **From:** "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state ma.us>
> > **Date:** February 23, 2022 at 1:13:12 PM EST
> > **To:** "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
> > **Subject: Re: Motorola meeting**
> >
> > No problem. Can you send me the email for the Motorola reps. I'll send an invite out with projected location.
> >
> > ---
> >
> > **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> > **Sent:** Wednesday, February 23, 2022 11:54 AM
> > **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> > **Subject:** Re: Motorola meeting

Great thanks Frank

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Sir,

I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 10:41 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:

Thank you. Fleet may send a representative or two.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 9:03 AM
To: Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
Cc: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
Subject: Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police

Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)"
<steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL)
<steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL)
<steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL)
> <steven mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

> On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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, thanks Captain. I'll just await a date that works best for you.
>
> Jim
>
> On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:
>
> > Sure Jim.
> >
> > Detective Captain Steven McCarthy
> >
> > Massachusetts State Police
> >
> > Division of Homeland Security and Preparedness
> >
> > 470 Worcester Rd
> >
> > Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State

Highway Patrol, Motorola
Public Safety Intelligence-Led
Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain
Steven McCarthy #1477

Executive Officer:
Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Cc: Driscoll, Francis (POL)
Subject: Re: Motorola meeting
Date: Wednesday, February 23, 2022 3:11:09 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.

Sure, here is the attendee list. Thank you!

sam.rabadi@motorolasolutions.com
jdowling@motorolasolutions.com
kevin.johnson3@motorolasolutions.com
daniel.wilburn@motorolasolutions.com
alan.melvin@motorolasolutions.com

Jim

On Wed, Feb 23, 2022 at 3:00 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> If you send me the team email addresses we will forward a calendar invite.
>
> Thanks
> Steve
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> Begin forwarded message:
>
> **From:** "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state.ma.us>
> **Date:** February 23, 2022 at 1:13:12 PM EST
> **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> **Subject: Re: Motorola meeting**
>
> No problem. Can you send me the email for the Motorola reps. I'll send an invite out with projected location.
>
> ---
>
> **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Sent:** Wednesday, February 23, 2022 11:54 AM
> **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> **Subject:** Re: Motorola meeting
>
> Great thanks Frank
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:

Sir,

I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 10:41 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Ok we might need to find a bigger space, maybe DFS conference room?

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

> On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us> wrote:
>
> Thank you. Fleet may send a representative or two.
>
> ---
>
> **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Sent:** Wednesday, February 23, 2022 9:03 AM
> **To:** Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
> **Cc:** Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
> **Subject:** Motorola meeting
>
> Good morning,
>
> Motorola good to go next Monday morning at GHQ.
>
> Respectfully,
> Steve
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> Begin forwarded message:
>
> > **From:** Jim Dowling <jdowling@motorolasolutions.com>
> > **Date:** February 22, 2022 at 6:43:16 PM EST
> > **To:** "McCarthy, Steven (POL)" <steven mccarthy@pol.state ma.us>
> > **Subject: Re: Follow Up**

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Tuesday, February 22, 2022 2:58 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
> **Subject:** Re: Follow Up
>
> 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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!
>
> Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, thanks Captain. I'll just await a date that works best for you.

Jim

On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Sure Jim.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com>

wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 470 Worcester Road
>
> Framingham, MA 01702
>
> 508-867-1052
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>

Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> I have no doubt Jim, thank you.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 7:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Cc: Driscoll, Francis (POL) <Francis.Driscoll@pol.state ma.us>; Pack, Noah (POL) <noah.pack@pol.state ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state ma.us>
Subject: Re: Follow Up

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, thank you for the additional details. I'll assemble the right technical resources so we can have a discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.

The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)

The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.

Thank you as always for your attention and assistance.

SM

Detective Captain Steven McCarthy #1477

Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven mccarthy@pol.state ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven mccarthy@state ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.
>
> There are two things you can help me with.
>
> The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.
>
> Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the

front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain Steven McCarthy #1477

Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last

week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

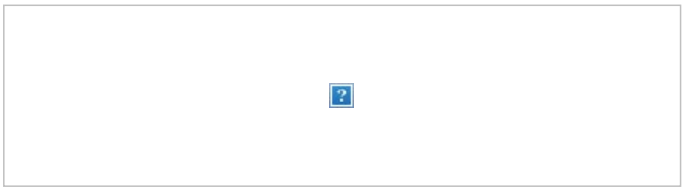


> *For more information on how and why we collect your personal information, please visit our Privacy Policy.*

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--
Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: Jim Dowling
To: McCarthy, Steven (POL)
Cc: Driscoll, Francis (POL)
Subject: Re: Motorola meeting
Date: Thursday, February 24, 2022 11:19:43 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.

Steve, sorry for the late add - we also have the following individual who will also attend. Thank you.

brady@motorolasolutions.com

Jim

On Wed, Feb 23, 2022 at 3:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Thanks Jim
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> On Feb 23, 2022, at 3:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
>
> 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.
>
> Sure, here is the attendee list. Thank you!
>
> sam.rabadi@motorolasolutions.com
> jdowling@motorolasolutions.com
> kevin.johnson3@motorolasolutions.com
> daniel.wilburn@motorolasolutions.com
> alan.melvin@motorolasolutions.com
>
> Jim
>
> On Wed, Feb 23, 2022 at 3:00 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
>
> > Hi Jim,
> >
> > If you send me the team email addresses we will forward a calendar invite.
> >
> > Thanks
> > Steve
> >
> > Detective Captain Steven McCarthy
> > Massachusetts State Police
> > Division of Homeland Security and Preparedness
> > 470 Worcester Rd
> > Framingham, MA 01702
> > 508-867-1052
> >
> > Begin forwarded message:
> >
> > **From:** "Driscoll, Francis (POL)" <Francis.Driscoll@pol.state.ma.us>
> > **Date:** February 23, 2022 at 1:13:12 PM EST
> > **To:** "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
> > **Subject: Re: Motorola meeting**

No problem. Can you send me the email for the Motorola reps. I'll send an invite out with projected location.

From: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Sent: Wednesday, February 23, 2022 11:54 AM
To: Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
Subject: Re: Motorola meeting

Great thanks Frank

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

> On Feb 23, 2022, at 11:40 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:
>
> Sir,
>
> I talked to Lt Brooks and we can use the Watch Center conference table. The HSOC main room should be empty and we could possibly use that also.
>
> ---
>
> **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Sent:** Wednesday, February 23, 2022 10:41 AM
> **To:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>
> **Subject:** Re: Motorola meeting
>
> Ok we might need to find a bigger space, maybe DFS conference room?
>
> Detective Captain Steven McCarthy
> Massachusetts State Police
> Division of Homeland Security and Preparedness
> 470 Worcester Rd
> Framingham, MA 01702
> 508-867-1052
>
> > On Feb 23, 2022, at 9:49 AM, Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us> wrote:
> >
> > Thank you. Fleet may send a representative or two.
> >
> > ---
> >
> > **From:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> > **Sent:** Wednesday, February 23, 2022 9:03 AM
> > **To:** Wilcox, Christopher (POL) <christopher.wilcox@pol.state.ma.us>; Murphy, Matthew G - DIS (POL) <matthew.g.murphy@pol.state.ma.us>; Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Nason, Nicholas (POL) <Nicholas.Nason@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Connor, Debora (POL) <Debora.Connor@pol.state.ma.us>
> > **Cc:** Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; JAMES DOWLING <jdowling@motorolasolutions.com>
> > **Subject:** Motorola meeting

Good morning,

Motorola good to go next Monday morning at GHQ.

Respectfully,
Steve

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
470 Worcester Rd
Framingham, MA 01702
508-867-1052

Begin forwarded message:

From: Jim Dowling <jdowling@motorolasolutions.com>
Date: February 22, 2022 at 6:43:16 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, we are good to go for 2/28. If we could schedule the session from 9:00am-11:00am, that would be appreciated. I can have boxed lunches brought in after our meeting if
that would be ok. Thanks again.

Jim

On Tue, Feb 22, 2022 at 3:42 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Probable attendees:
>
> Lt. Colonel Christopher Wilcox
>
> Major Matthew Murphy
>
> Det. Captain Steve McCarthy
>
> Lieutenant Francis Driscoll
>
> Sergeant Noah Pack
>
> Sergeant Nicholas Nason
>
> Mr. Brian Egnitz
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Executive Officer: Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 22, 2022 2:58 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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.

Steve, when you have a chance, could you provide the titles of the MSP attendees. I'll circle back soon to confirm if 2/28 works. Thanks again.

Jmi

On Tue, Feb 22, 2022 at 9:25 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Good morning Jim,
>
> Looks like next Monday (2/28), is going to be the best day for the MSP team, hopefully that works for you and your folks.
>
> Let me know,
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Monday, February 21, 2022 1:07 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Subject:** Re: Follow Up

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 Captain, hope you had a nice weekend. I was just checking in to see if you had decided on a date. Thanks!

Jim

On Wed, Feb 16, 2022 at 9:28 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Should have it soon.
>
> Detective Captain Steven McCarthy
>
> Massachusetts State Police
>
> Division of Homeland Security and Preparedness
>
> 470 Worcester Rd
>
> Framingham, MA 01702
>
> 508-867-1052
>
> > On Feb 16, 2022, at 9:11 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:
> >
> > 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, thanks Captain. I'll just await a date that works best for you.
> >
> > Jim
> >
> > On Wed, Feb 16, 2022 at 9:09 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:
> >
> > > Sure Jim.
> > >
> > > Detective Captain Steven McCarthy
> > >
> > > Massachusetts State Police
> > >
> > > Division of Homeland Security and

Preparedness

470 Worcester Rd

Framingham, MA 01702

508-867-1052

On Feb 16, 2022, at 9:08 PM, Jim Dowling <jdowling@motorolasolutions.com> wrote:

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, is it possible to have an initial meeting with just you to have a higher level discussion and then return with our techies to delve into the technical details? That is our initial thought if that works for you.

Jim

On Wed, Feb 16, 2022 at 3:25 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'm checking with our people and should have a date for you shortly, looks like Tuesday is out, probably going to be Wednesday (3/2), but I'll know for sure in the next day or two.
>
> SM
>
> Detective Captain Steven McCarthy
>
> Division of Homeland Security and Preparedness

Massachusetts State Police

470 Worcester Road

Framingham, MA 01702

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Tuesday, February 15, 2022 8:39 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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 Captain, I am just following up per your request to see if you are free the week of 2/28 to have an initial discussion about the technology topics you mentioned. I am thinking the first meeting would be with just you to discuss MSP's requirements and goals along with a executive level discussion about ALPR, mobile video, and the "connected cruiser". I will have two individuals with me who are very knowledgeable on these topics and have a lot of experience with these technologies on the law enforcement side, both at the state and federal level (brief summary below). I thought we could meet in the morning from 9-11am and then have lunch if your schedule permits. Thanks.

Sam Rabadi: Former Secret Service Agent, ATF Special Agent in Charge (ret.), Senior Consultant Motorola Intelligence-Led Public Safety Team

Alan Melvin: Lieutenant Colonel / Director of Support Operations (ret.) - NC State Highway Patrol, Motorola Public Safety Intelligence-Led Public Safety Team

Jim

On Thu, Feb 3, 2022 at 7:35 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> I have no doubt Jim, thank you.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness
>
> Massachusetts State Police
>
> 508-867-1052
>
> ---
>
> **From:** Jim Dowling <jdowling@motorolasolutions.com>
> **Sent:** Thursday, February 3, 2022 7:34 PM
> **To:** McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
> **Cc:** Driscoll, Francis (POL) <Francis.Driscoll@pol.state.ma.us>; Pack, Noah (POL) <noah.pack@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** Re: Follow Up
>
> 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, thank you for the additional details. I'll assemble the right technical resources so we can have a

discussion about each of those areas.

Jim

On Thu, Feb 3, 2022 at 7:10 PM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> I'll check with the rest of the team and get back to you soon.
>
> The 4RE issue is looking at the logistics that surround using 4G to upload the video. To the best of my understanding the equipment we have would allow that if coupled with the necessary 4G router in the cruiser. It's part of a larger look at the best way to approach cellular mobility in a cruiser coupled with the growing number of devices that need/could benefit from mobile connectivity. (i.e. mobile computing, AVL traffic, LPR, in-car video)
>
> The Vigilant conversation is so the team can take another look at the Motorola offerings, so we can fully consider the solutions available as we roadmap out our LPR strategy.
>
> Thank you as always for your attention and assistance.
>
> SM
>
> Detective Captain Steven McCarthy #1477
>
> Division of Homeland Security and Preparedness

Massachusetts State Police

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Thursday, February 3, 2022 6:34 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Re: Follow Up

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, could you let me know your availability next week for a call or two on the topics you referenced in your email? Thanks.

Jim

On Wed, Feb 2, 2022 at 11:55 AM McCarthy, Steven (POL) <steven.mccarthy@state.ma.us> wrote:

> Hi Jim,
>
> Sorry for the delay in responding.
>
> Thank you very much for your outreach. Kevin did tell me of his retirement, he will be missed as he was always very responsive and an able representative for Motorola.
>
> I am sure his successor will be as well, and I look forward to meeting them when they are available.

There are two things you can help me with.

The first is Kevin had set up a meeting with to discuss both Vigilant and sending 4RE video out via 4G. Unfortunately, COVID interfered and struck down part of your team. We are still interested in discussing these issues and would like to setup a virtual meet this month if possible.

Two, there's been interest here in having a lanyard type mount for the V300 for some of our plainclothes officers. I've attached a photo of one I cobbled together from a broken mag clip. It's the front mount plate coupled with an adjustable breakaway mask lanyard. Would it be possible, presuming the order was sufficiently large, to obtain the front plate only sans magnets and levers, so we could fashion some of these mounts?

Also, I've attached a Word version of the BWC policy for you to forward to the requesting agency.

Thanks,

SM

Detective Captain
Steven McCarthy #1477

Executive Officer:
Planning, Preparedness, and Response Section

Massachusetts State Police

Division of Homeland Security and Preparedness

508-867-1052

From: Jim Dowling <jdowling@motorolasolutions.com>
Sent: Monday, January 31, 2022 7:11 PM
To: McCarthy, Steven (POL) <steven.mccarthy@pol.state.ma.us>
Subject: Follow Up

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 Captain, I just wanted to reach out as I understand that Kevin Coughlin had contacted you about his retirement last week. I expect his replacement will be announced in a few weeks. I will certainly set up a brief call with an introduction in Feb. If there is anything I can do to provide any assistance in the interim, please feel free to contact me.

I also wanted to ask if you may be able to forward a copy of the MSP body worn program policy. Another state agency in MA is considering use of BWCs and asked me if I could provide policy info. Thank you.

Jim

--

Jim Dowling
Account Manager

Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Account Manager
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

--

Jim Dowling
Senior Account Executive
Motorola Solutions, Inc.

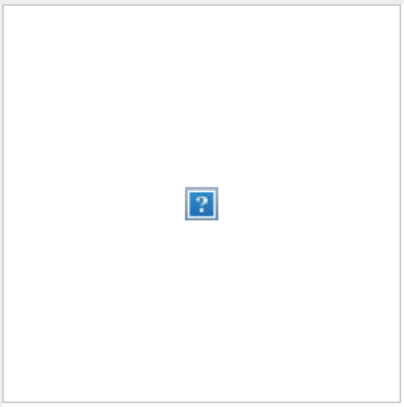
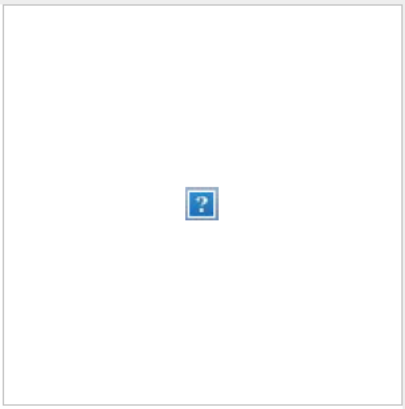
M. 513-292-0805
E. jdowling@motorolasolutions.com

The 1st In-Car Video System Enabled By Artificial Intelligence. Learn More.



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

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: Webinar: ALPR: Addressing misconceptions and key considerations to select the best solution for your community
Date: Wednesday, October 19, 2022 11:31:15 AM

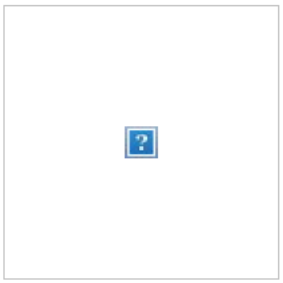

Register Now!

Automatic License Plate Recognition (ALPR) is an effective and intelligent tool to keep communities safe; however, there are many misconceptions amongst law makers and the communities they represent about how the technology works, how it is operated and how it impacts privacy. With the proliferation of this misinformation, it is becoming increasingly difficult for law enforcement to communicate that ALPR is a force for good that helps protect the communities they serve.

We're bringing together Lawrence Police Department Chief Gary Woodruff along with ALPR expert Andy Jessen of Utility to share insight into how to address misconception and misinformation about ALPR technology, as well as key considerations to select the right technology to allay community concerns and serve as a force multiplier. Join us to for key learnings including:

- An overview of LPR/ALPR technology of the past, present and future
- How to address common misconceptions about and unique community needs for ALPR, including privacy concerns and response times
- Key insights to consider when selecting ALPR technology
- The benefits of effective ALPR technology for agencies, district attorneys and communities
- Real-life examples of how ALPR technology supports agencies and communities





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

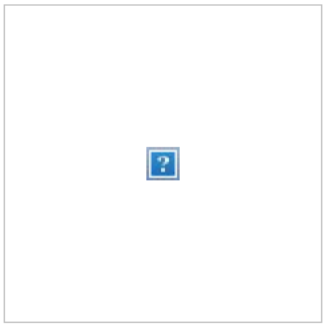
You can edit your Communication Preferences from your Profile on the FBINAA Website.

FBI National Academy Associates, Inc. | FBI Academy, Building 8-102, Quantico, VA 22135

Unsubscribe steven.mccarthy@pol.state.ma.us

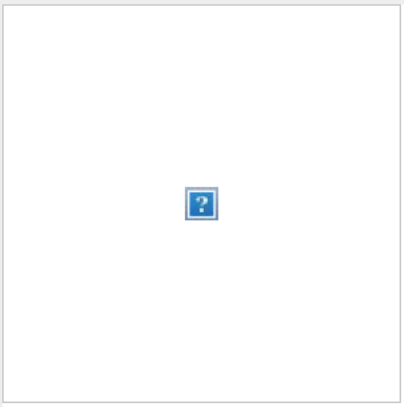
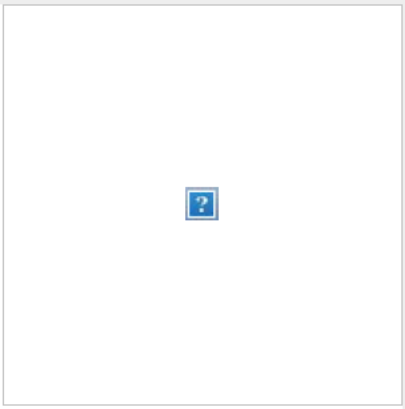
Constant Contact Data Notice

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: ALPR: Addressing misconceptions and key considerations to select the best solution for your community
Date: Thursday, October 27, 2022 10:21:05 AM

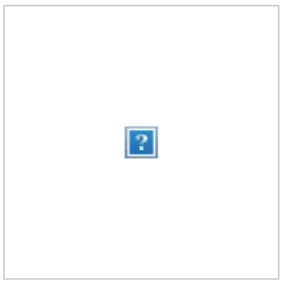

Register Now!

Automatic License Plate Recognition (ALPR) is an effective and intelligent tool to keep communities safe; however, there are many misconceptions amongst law makers and the communities they represent about how the technology works, how it is operated and how it impacts privacy. With the proliferation of this misinformation, it is becoming increasingly difficult for law enforcement to communicate that ALPR is a force for good that helps protect the communities they serve.

We're bringing together Lawrence Police Department Chief Gary Woodruff along with ALPR expert Andy Jessen of Utility to share insight into how to address misconception and misinformation about ALPR technology, as well as key considerations to select the right technology to allay community concerns and serve as a force multiplier. Join us to for key learnings including:

- An overview of LPR/ALPR technology of the past, present and future
- How to address common misconceptions about and unique community needs for ALPR, including privacy concerns and response times
- Key insights to consider when selecting ALPR technology
- The benefits of effective ALPR technology for agencies, district attorneys and communities
- Real-life examples of how ALPR technology supports agencies and communities





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

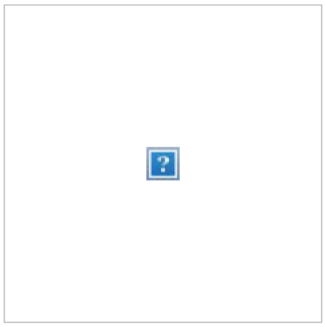
You can edit your Communication Preferences from your Profile on the FBINAA Website.

FBI National Academy Associates, Inc. | FBI Academy, Building 8-102, Quantico, VA 22135

Unsubscribe steven.mccarthy@pol.state.ma.us

Constant Contact Data Notice

Sent by do-not-reply@fbinaa.org in collaboration with



Try email marketing for free today!

From: Vetted Info
To: Egnitz, Brian (POL)
Subject: Who Is Vetted Security Solutions?
Date: Thursday, June 9, 2022 5:40:30 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.

Cutting EDGE CRIME



Vetted Security Solutions

Vetted Security Solutions provides comprehensive solutions that enable public safety entities to prevent and solve crimes. Offering industry-leading manufacturers, as a single-source solutions provider Vetted can design, manufacture, install, and provide post-deployment support.

Our vast technology offering includes Fixed, Mobile, and Trailer ALPR systems,

facial recognition, video analytics, and more safety and surveillance solutions. For more than a decade, Vetted has proudly served law enforcement agencies, municipalities, commercial and Academic campuses with cutting-edge crime-fighting solutions for a safer community.

The VETTED ADVANTAGE

Needs assessments, site planning, and implementations are stressful enough without adding the complications of multiple service providers. As a premier integrator, Vetted provides support and management during all phases of the project.

LEARN MORE

Automated License Plate Recognition (ALPR)

Vetted's ALPR solutions include Fixed, Mobile, and Trailer systems to scan vehicles at various speeds to provide critical investigative data.





CCTV & Surveillance

Take your surveillance to the next level with Vetted's industry-leading optic solutions designed for day and night imaging.

Video Analytics

You can capture quality imaging, but what you do with the data is what matters. Transform your data into actionable intelligence.



Data Aggregation

finder



Link and share data with the most advanced information sharing and investigative lead generation platform for law enforcement.

Facial Recognition

Rapidly generate leads with facial recognition to identify suspects, witnesses, and victims to close cases faster than ever.

3



Contact Us to learn how you can benefit from Vetted's Cutting Edge Crime Fighting Solutions.

CONTACT US

Vetted Security Solutions, 4185 35th St N, St Petersburg, FL 33714, USA, 727 440 3245

Unsubscribe Manage preferences

From: Scott Pearson
To: McCarthy, Steven (POL)
Subject: whooster
Date: Tuesday, July 5, 2022 11:05:08 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.

Sir,

I am a manufacturer's representative for Whooster / OWL (public - private data sources) and would like to set up a time to discuss.

OWL's resident AI technology provides a single platform to manage, execute and analyze all your digital assets.

Talega Technology represents:

Thomson Reuters Clear (LPR data only)

Vetted Security Solutions (ALPR)
www.vettedsecuritysolutions(dot)com

Finder (records sharing)
www.findersoftware(dot)com

Whooster / OWL (public - private data sources)
www.whooster(dot)com &_www.owlintel(dot)ai

Geolitica (data for proactive crime policing)
www.geolitica(dot)com

v/r,

Scott Pearson
703-598-1238

Handfield, Kenneth (POL)

From: Handfield, Kenneth (POL)
Sent: Monday, December 28, 2020 3:25 PM
To: Slater, Michael (POL); Ross, Jonathan (POL); Gleason, Kristin (POL)
Subject: LPR Access

Do your centers have access to any LPR systems other than the 3M/BOSS/Newology that we were using? (e.g. FLOCK.)

~K

Kenneth E. Handfield, Jr.
Director of Dispatch Services

Massachusetts State Police, Headquarters
470 Worcester Road
Framingham, MA 01702

Office: 508.820.2347
Fax: 508.820.2359
Cell: [redacted]

Email: Kenneth.Handfield@Mass.gov

Handfield, Kenneth (POL)

From: Handfield, Kenneth (POL)
Sent: Monday, December 28, 2020 3:27 PM
To: Barstow, Matthew (POL)
Subject: LPR Access

Hey- just want to give you a heads up. I spoke with Jen Staples and we thought it would be prudent to instruct our communications centers that had LPR accounts provided by neighboring agencies to hold off using any LPR software until we how ubiquitous this time mismatch issue is. (Not sure if it is unique to Newology or broader.)

~K

https://www.bostonglobe.com/2020/12/23/metro/after-finding-glitch-massachusetts-suspends-use-controversial-camera-system-that-lets-police-track-cars/?outputType=amp

I guess they shut us down!

M E M O R A N D U M

From: Executive Office of Public Safety and Security

To: Criminal Justice Agencies and Criminal Defense Counsel in the Commonwealth of Massachusetts

Date: December 23, 2020

Re: Notice of ALPR Date/Time Reliability Issue

To Whom It May Concern:

This memorandum is intended to inform all criminal justice agencies and criminal defense counsel in the Commonwealth of Massachusetts of an issue regarding the reliability of date and time stamps from Automatic License Plate Reader ("ALPR") cameras used by the Massachusetts State Police ("MSP") and sourced from vendor Neology, Inc. ("Neology"). This memorandum applies to MSP ALPR cameras that are currently in a fixed position or can be moved to a fixed position. It does not apply to cruiser-mounted ALPR cameras.

The Executive Office of Public Safety and Security ("EOPSS") and MSP hereby notify all criminal justice agencies and criminal defense counsel that, for the reasons provided below and until further notice, a date and time recorded by a Neology ALPR camera in a fixed position between May 2015 to November 12, 2020, should not be relied upon in the absence of information supporting the accuracy of that date and time, such as upload date and time information recorded by the host server or other corroborative evidence.

The ALPR system is composed of a network of high-speed cameras located throughout the Commonwealth. The cameras in the network use computer algorithms capable of converting the images of license plates into electronically readable data. The ALPR records the date, time, and location that a car passes, and the camera takes a photograph of the license plate. The information and photograph are quickly uploaded to host servers at the Public Safety Data Center in Chelsea, and the host servers record the date and time of that upload. Those servers support a searchable database of the license plate data that is maintained by the Executive Office of Public Safety and Security. The information in the database is available to law enforcement agencies conducting criminal investigations.

In November 2020, while reviewing ALPR data, MSP discovered instances where the dates and times recorded by ALPR cameras did not align with the dates and times those photographs were uploaded to the cameras' host servers. MSP, working with Neology, has determined that these particular time gaps occurred when an ALPR camera that lost power reconnected with its power source and began taking pictures prior to connecting with its host server. During the time period after the ALPR was powered on, but before it connected with the host server, the ALPR could not update its date and time settings to the correct time. Once the ALPR connected with its server, its date and time settings were synchronized with the host server.

As a result, in any case where the ALPR lost power, the ALPR could have inaccurately recorded the date or time on which the picture was taken if that picture was taken prior to the ALPR establishing a connection with the host server. The issue is limited to the date and time recorded by the ALPR camera and not to the license plate data itself. The date and time of upload recorded by the host server is accurate and unaffected by this issue. Therefore, a comparison between the date and time recorded by the ALPR on the image and that recorded by the host server can indicate whether the ALPR-recorded information is accurate. For example, that accuracy might be shown where the time recorded by the ALPR camera is close in time to that recorded by the host server. Such comparison data is generally available from November 20, 2019, through the present, as a Department of Criminal Justice Information Services ("DCJIS") policy required MSP to retain that data for one year.

Shortly after learning of this issue on November 12, 2020, MSP suspended the use of fixed-position ALPR cameras and preserved all existing ALPR data. MSP will continue to preserve all ALPR data and fixed-position ALPR cameras will not be utilized until further notice. EOPSS and MSP will continue to work with Neology to address this issue and will provide updates.

To request server upload date and time data, please contact ALPRVerify@Mass.gov

Handfield, Kenneth (POL)

From: Handfield, Kenneth (POL)
Sent: Tuesday, December 28, 2021 1:09 PM
To: Demers, Joanne (POL)
Subject: FW: LPR Access / DSU

Joanne,

All LPR queries can be run through Fusion/Watch until the next iteration of the plate reader software is made available and our access approved through chain-of-command to the Division Commander of Homeland Security. However, if we find that some of our personnel still have access to 3M/Boss, they should only be accessing the LPR for real-time incidents. Under no circumstances should they be creating or modifying alerts or hotlist entries without the oversight of Fusion/Watch.

Thanks,
Ken

From: Pack, Noah (POL) <noah.pack@pol.state.ma.us>
Sent: Tuesday, December 28, 2021 9:40 AM
To: Handfield, Kenneth (POL) <kenneth.handfield@pol.state.ma.us>
Subject: Re: LPR Access / DSU

Hi Ken,

The Department's LPR system is partially back online. Any users who had accounts previously are able to access the system using the same credentials. We are in the process of transitioning to a new system in the coming months, and we will be in touch as that moves forward. We are not setting up new accounts in the old system at this time.

Please ensure that all historical query requests are directed to the Commonwealth Watch Center, which will ensure appropriate search procedures and tracking. The Watch is also available to assist with real-time queries and hotlist entries for BOLOs etc. Thank you for your interest, and Happy New Year.

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

Bringing Safer Streets to Your City



STALKER
STREET DYNAMICS

BUY AMERICA ACT
STALKER
COMPLIANT

THE SOFTWARE



STREET DYNAMICS PORTAL

Remotely access your speed feedback signs (PMGs). Program messages, create a schedule, and generate traffic data reports



EASY ANALYST SOFTWARE

Create traffic reports from any Street Dynamics Product with the Traffic Statistics Package

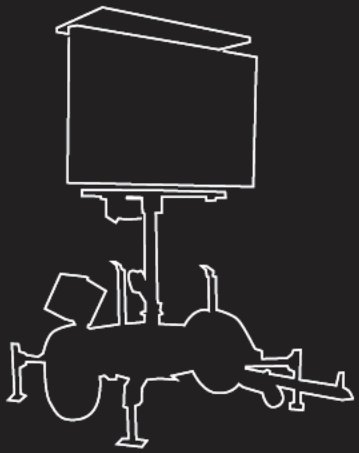
THE ALL-IN-ONE



POLE MOUNTED FULL MATRIX GRAPHIC DISPLAY (PMG)

Slow down traffic, display messages, and collect traffic data

SPEED A



MESSAGE CENTER 360

The largest display for your most important messages

ISO 9001:2015 Certified TRC

MUTCD Compliant

NTCIP Compliant

BUY AMERICA ACT STALKER COMPLIANT

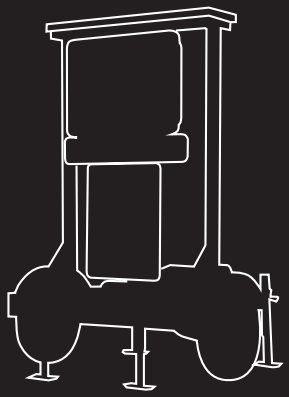
The Safest Choice

You rely on law enforcement officers to keep your community safe. Unfortunately, they can't keep watch over every road, neighborhood, school zone, and construction area 24/7/365.

Our radar speed signs and messaging trailers, however, never move, never sleep, and never stop monitoring your streets for safety.

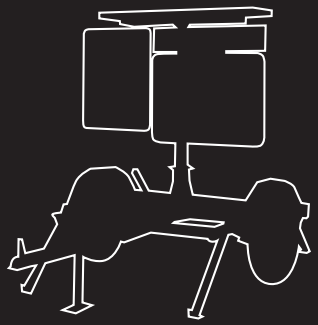
Stalker Radar technology is at the core of Street Dynamics, ensuring that your residents are protected by the most accurate and reliable street safety equipment available on the market today.

ND MESSAGING TRAILERS



SPEED AWARENESS MONITOR (SAM)

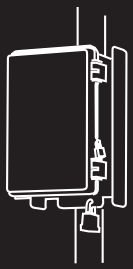
A take-anywhere radar speed feedback trailer with a changeable speed limit sign



SAM-R

Speed readings without the hassle, featuring a rotating mast design for easy setup and towing

SHOW ME THE NUMBERS



TRAFFIC DATA COLLECTOR (TDC)

Covertly track vehicle speeds and traffic patterns

DID YOU KNOW?

Street Dynamics signs are powered by Stalker Radar- the same legendary radar technology used by over 85% of all Municipal, County, and State Police agencies.

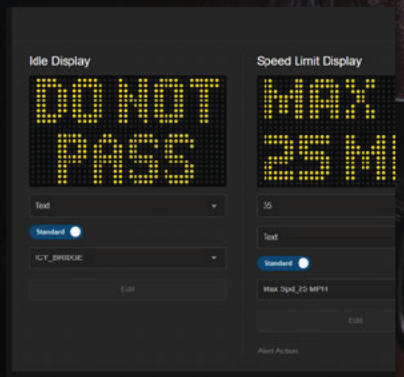
STREET DYNAMICS PORTAL

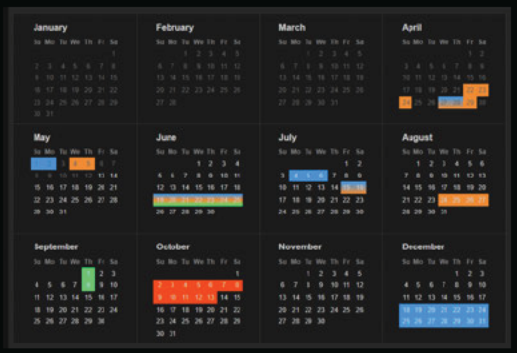
PMG

Create custom text messages and graphics

The intuitive interface of Street Dynamics allows you to start creating text messages and graphics as soon as you log in to the portal. You can even arrange collections of these messages into looping sequences that convey more information than you can display on a single screen.

And to help you get started even faster, Street Dynamics comes pre-loaded with a wide variety of standard messages that you can start using with the click of a button.





Schedule messages to appear on your sign months or even years in advance

It is easy to assemble and schedule a sequence of messages and graphics to display on your PMG. The color-coded interface makes it easy to see at a glance exactly when your messages will appear.

"When road conditions change, so can our signs

Publish detailed reports from your traffic data

Your PMG collects traffic data 24/7. Our easy-to-configure reports turn these datapoints into useful, actionable information that you can use to guide enforcement efforts, observe driver behavior, and understand traffic patterns.

Combine multiple reports and charts to convey the exact information that you need to share with your agency, city, HOA, or other stakeholders. Print reports as PDFs or email them to an unlimited number of people.

The Web Portal to Safety

The Street Dynamics Web P rtal offers the convenience of re otely accessing all your connected PMGs



- right from my desk"

STALKER
STREET DYNAMICS
TRAFFIC DATA INTELLIGENCE



PMG



MC360



SAM



SAM-R



MC 360

ig Messages ith Big Impact

Get the attention of any driver with the MC360 - our largest messaging trailer. Available with or without radar speed tracking technology.



SAM

The SAM and SAM-R trailers are tough and durable while also being easy to move and quick to set up. They both feature speed limit signs with changeable numbers so they can be used on any street.

Put a Speed Sign Right Where You Need It



SAM-R



Slower Streets are Safer Streets

Radar speed signs and messaging trailers have been shown to consistently lower average traffic speeds by up to 9 MPH, and the effect lasts even years after the sign has been installed. Use them in school zones, work zones, transition zones between areas of high and low speeds, in parking lots, at events, and more.

"People are driving too fast in my neighborhood"



PMG

The PMG is our most versatile, all-in-one traffic calming device

- A radar speed sign that measures and display drivers' speeds
- A messaging sign that displays text messages and graphics
- A traffic data collector that captures and stores vehicle speed and traffic information internally or uploads it to the Street Dynamics Web Portal

DID YOU KNOW?

Speed is one of the top three contributors to traffic fatalities.

The PMG is the only NTCIP-Compliant radar speed sign available on the market today.



STREET DYNAMICS PORTAL



PMG



FLOOD SENSOR

Save Lives *(and resources)* with the PMG Flood Sensor

Many communities have “problem areas” where flooded roadways are more l kely to occur. Rather than manually monitoring each street, you can use our Flood Sensor to automatically trigger your PMG to display alerts such as “HIGH WATER”, “FLOOD AREA”, “ROAD CLOSED”, or any other customized message desired.

Up to 3 Flood Sensors can be attached to a single PMG, giving you the ability to escalate and de-escalate messages automatically as waters rise and recede.





PMG Flood Sensor
Automatically Detects High Water

"We can't monitor all

Not Just for City Streets

The Flood Sensor is great for notifying motorists about water on the road, but it is also perfect for keeping hikers, boaters, rafters, and other park visitors safe. Pair your PMG with optional solar panels for infinite operation.

In Case of Emergency

Welcome to the world of automated safety

Faster and clearer communication is key to creating more safety in your community, but when emergencies arise, you don't always have the time or resources available to spread the word.

Automation and remote access options allow Street Dynamics to handle your road safety so you can focus on everything else.



Trigger Warning

GPIO triggers expand the capabilities of your PMG. Now you can set up NTCIP-compliant "WRONG WAY" alerts - complete with strobes - for one-way streets and highway off-ramps, or you can automatically display a "STOP" message any time your fire trucks or emergency vehicles go out on a call.

of our flood zones at once, but Street Dynamics can"





Lead the Way

For a truly mobile alert system, pair a PMG with our hitch mount. Now your sign can go anywhere your vehicle can.

Instant Messaging

Change your PMG at a moment's notice using the Street Dynamics Web Portal. You can even use the Calendar feature to display a message for a specific amount of time, reverting to "regularly scheduled programming" automatically afterwards.



MC360



SAM



SAM-R

A Big Deal

Our flagship Messaging Trailer, the MC360 is capable of conveying any message you need to send. Its full-matrix MUTCD-compliant amber LED display is visible from up to 1,000 feet, and you can choose from four different sizes to suit your needs.

Crafted from durable steel and finished with rust- and graffiti-resistant paint in your choice of color, the MC360 can be customized with a variety of options, including:

- Radar speed detection
- Traffic data and statistics package
- Strobes
- Solar power
- ALPR/ANPR-ready
- Web-based remote access
- NTCIP- and MUTCD- compliant



When you really need to get drivers' attention

Big Problems Require Big Solutions

They Could Be Anywhere

Drivers don't just speed on one street and then choose to drive safely everywhere else. Having the ability to quickly move your radar speed signs to trouble-spots around your city is a game-changer. The SAM and SAM-R are compact enough that they can be easily towed and set up by just one person.



SAM

signs really do slow down traffic and make us safer"



Take It (Really) Slow

Some locations, such as warehouses, supply yards, boarding "no wake" areas, and other low speed, high-risk environments, need extra-slow speeds to ensure safety.

The new Low-Speed PMGs sensors are fine-tuned to be triggered by speeds as slow as 1 MPH.



SAM-R

TDC

EASY ANALYST

PMG

Hidden in Plain Sight

Traffic Data Collector (TDC)



Collect traffic data based on how drivers ***actually*** behave when they think that no one is watching. Load collected data into the included Stalker Easy Analyst software to create reports, charts, and graphics.

Runs for up to 7 days on battery power or choose the solar panel option for infinite field operation

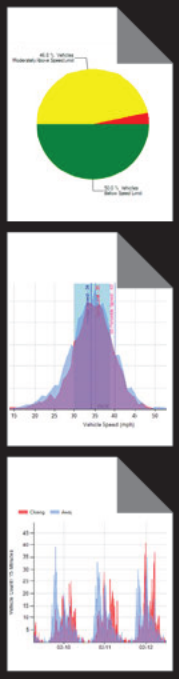
The tamper-proof, lockable, and durable non-corroding housing mounts to any pole.

Reporting for Duty

Easy Analyst Software

The Stalker Easy Analyst software offers the same reporting capabilities as Street Dynamics for all of our traffic data-collecting speed signs and messaging trailers. Simply download the traffic data from your sign onto a USB thumb drive, upload it into Easy Analyst, and, in just a few clicks, create the reports and graphs you need.

It's as easy as 1, 2, 3.





PMG



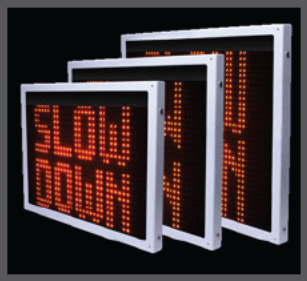
Add Solar

Multiple Surround Options

Choose Your Mounting Kit



Wireless Application



Available in 3 character heights: 12", 15", and 18"

Power	Solar	optional
	Battery Power	optional
	Direct DC	optional
	AC	●
Radar	Band	K
	Detection Distance	up to 900 ft.
Setup + Traffic Data Analysis	Street Dynamics Web Portal	optional
	Speed Sign iOS and Android Apps	●
	Easy Analyst Software	●
	PC Application	●
	Short Range Wireless	optional
Mounting + Towing	Pole Mount	optional
	Trailer Mount	*see Mini-Message Trailer*
	Vehicle Hitch Mount	optional
	Handle + Feet	optional
Sign Visibility *(Distance)*	18" model	up to 900 ft.
	15" model	up to 750 ft.
	12" model	up to 600 ft.
Message Display Types	Speed	●
	Text and Graphics	optional
	Moving Animations	optional
Compatibility	MUTCD	●
	NTCIP	optional
Upgrades	Simulated Camera Flash	optional
	Strobes	optional
	External Input / Triggers	optional
	Low Speed Model	optional
	Flood Sensor	optional

Available Options:



Flood Sensor



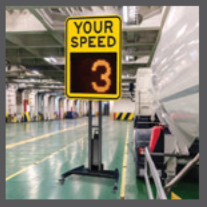
Solar Power



Hitch Mount



GPIO Connections



Low-Speed Model



Battery Backpack

FEATURED PRODUCTS



MC360



SAM



SAM-R



PMG



MC 360



4' x 8' Display



3' x 6' Display



SAM

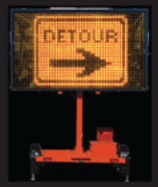


SAM-R

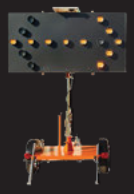
ALSO AVAILABLE



3-Line Display
70" x 127" Display



Full Matrix Trailer
79.5" x 133" Display



15 and 25 Light
Arrow Boards

Options

	MC360	SAM	SAM-R
POWER			
Solar	optional	optional	optional
Battery Power	●	●	●
AC	charging	charging	charging
SETUP + TRAFFIC DATA ANALYSIS			
Remote Access	optional		
Easy Analyst Software	optional	optional	optional
COMPATIBILITY			
MUTCD	●	●	●
NTCIP	●		
RADAR			
Band	K-Band (optional)	K-Band	K-Band
Detection Distance	up to1,200 ft. (opt.)	up to 1,200 ft.	up to 1,200 ft.
MOUNTING + TOWING			
Trailer Mount	●	●	●
Removable / Folding Tongue		●	●
Rotating Sign and/or Mast	●		●
DISPLAY OPTIONS			
Speed	optional	●	●
Text and Graphics	●		
Moving Animations	●		
SIGN VISIBILITY			
Distance	up to 850 ft./ (4'x8' size)	1000 ft.	1000 ft.
UPGRADES			
Strobes	optional	optional	optional
ALPR / ANPR Ready	optional		
Traffic Data Collection	optional	●	●



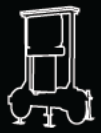
STREET DYNAMICS PORTAL



PMG



MC360



SAM



SAM-R



TDC

StreetDynamics.com

U.S. Sales

1-800-782-5537

MUTCD Compliant

NTCIP Compliant

applied concepts, inc.
855 East Collins Boulevard ■ Richardson, Texas 75081
972.398.3780 ■ Fax 972.398.3781

ISO 9001:2015 Certified

© 2022 Applied Concepts, Inc. All Rights Reserved. Specifications subject to change.

006-0075-00 Rev A



MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MassDOT)
10 PARK PLAZA
BOSTON, MA 02116

REQUEST FOR RESPONSE (RFR)

Equipment, Parts & Services for Telecommunications, ITS, IPCS Systems

COMMBUYS Bid: BD-20-1030-0P100-0P070-49476
Project Info #: 111753

Date: Revised 9 July 2020

Rolling Enrollment: ***Bidders may submit qualifications response at anytime***

Please Note: This is a single document associated with a complete Bid (also referred to as Solicitation) that can be found on www.COMMBUYS.com. All Bidders are responsible for reviewing and adhering to all information, forms and requirements for the entire Bid, which are all incorporated into the Bid. Bidders may also contact the COMMBUYS Helpdesk at COMMBUYS@state.ma.us or the COMMBUYS Helpline at 1-888-MA-STATE. The Helpline is staffed from 8:00 AM to 5:00 PM Monday through Friday Eastern Standard or Daylight time, as applicable, except on federal, state and Suffolk county holidays.

1 RFR INTRODUCTION AND GENERAL DESCRIPTION 1

1.1 Procurement Scope and Description 1
1.2 Background Information 1
1.3 Applicable Procurement Law 1
1.4 Number of awards 1
1.5 Adding Contractors after Initial Contract Award 1
1.6 Eligible Entities 1
1.7 Acquisition Method(s) 2
1.8 Contract Duration 2
1.9 Estimated Value of the Contract 2

2 ESTIMATED PROCUREMENT CALENDAR 3

2.1 Amendment Deadline 3

3 SPECIFICATIONS 3

3.1 Project Goal 3
3.2 Funding of Contract 4
3.3 Confidentiality and Security of Data 5
3.3.1 Pricing 5
3.4 Payment 5
3.5 Subcontracts 5
3.6 Bidder's Liability 6
3.7 Contract Management (Service Provider's interface with MassDOT's Contract Manager) 6
3.8 Vendor Warranty 7

4 AUDIT 7

5 EVALUATION CRITERIA 7

6 BID QUALIFICATIONS 8

7 FORMS 9

7.1 Supplier Diversity Program 10

8 HOW TO SUBMIT A RESPONSE 11

9 REQUIRED TERMS 12

9.1.1 Alterations 12
9.1.2 Ownership of Submitted Quotes 12
9.1.3 Prohibitions 12
9.2 Terms and Requirements Pertaining to Awarded Contracts 13
9.2.1 Commonwealth Tax Exemption 13
9.2.2 Vendor Contact Information 13
9.2.3 Publicity 13
9.2.4 Standards of Performance and Qualifications 13

10 INSURANCE 14

11 OTHER SPECIFICATIONS 16

12 MASSDOT TELECOMM RESPONSE FORM – 19

1 RFR INTRODUCTION AND GENERAL DESCRIPTION

1.1 Procurement Scope and Description

The Massachusetts Department of Transportation (MassDOT) seeks vendors to provide specialized Equipment, Parts & Services for MassDOT's Transportation and Roadway Telecommunications, Intelligent Traffic systems (ITS), Integrated Project Control Systems (IPCS).

1.2 Background Information

MassDOT operates a wide array of transportation systems throughout the Commonwealth, many of which are integrated with Federal and neighboring states. Key Telecommunications, ITS, IPCS Systems are in place to keep these systems running efficiently, providing a safe system for all users. MassDOT seeks to place pre-qualified vendors under Master Service Agreement contracts to supply equipment, parts, and services for the systems in place as well as replacement systems potentially needed in future years, within the terms of this solicitation. See Section 3.0 below.

NOTE: MassDOT monitors closely products and vendors available through statewide contracts managed by the Operational Services Division (OSD)[1]. MassDOT does not seek to replace product or vendors currently available through OSD statewide contracts by this solicitation.

1.3 Applicable Procurement Law

This Bid is issued under the following laws: MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00

1.4 Number of awards

MassDOT intends to make a **MULTIPLE** awards.

1.5 Adding Contractors after Initial Contract Award

If, over the life of the Contract, MassDOT determines that additional contractors should be added, these may be drawn from qualified companies which responded to this solicitation but were not awarded contracts. If necessary to meet the needs of MassDOT, the solicitation may be reopened to obtain additional responses from interested vendors

1.6 Eligible Entities

~~Any contract resulting from this Bid will be open for use by **MassDOT** only.~~

Any contracts resulting from this RFR may be used by **all departments of MassDOT**, the Commonwealth, including all constitutional offices, the legislature, and the judiciary; cities, towns, municipalities, counties, and other political subdivisions of the Commonwealth, including schools, and other service districts; authorities, commissions, institutions of higher education, and quasi-public agencies, and Not for Profit contractors currently contracting with the Commonwealth to provide human and social services; and other eligible entities designated in writing by the State Purchasing Agent. All entities other than MassDOT must execute a separate contract that meets their own legal and business requirements.

[1] https://www.mass.gov/service-details/find-a-statewide-contract-user-guide

1.7 Acquisition Method(s)

This solicitation is for the pre-qualification of suitable vendors. Subsequent acquisitions from selected vendors will be through the purchase of goods and/or services.

1.8 Contract Duration

Contract Duration	Number of Options	Number of Years	Instructions
Initial Duration	N/A	Up to 5	The contract will be executed for this initial duration and will begin on the contract start date.
Renewal Options	2	Up to 3	Two options to renew for three years each.
Total Maximum Contract Duration		Up to 11	

Each contractor's performance will be evaluated on an ongoing basis and will be utilized in determining whether or not to exercise any option to renew. Renewal of contracts will be at the discretion of the agency and subject to a performance evaluation. This evaluation may include, but not limited to, the following criteria:

- Vendor has performed well on project assigned
- Vendor provided a key individual to serve as a liaison and provided contact information
- Vendor responds to agency inquiries on a timely basis
- Vendor communication is clear and helpful
- Vendor files invoices and reports on a timely basis
- Vendor skill sets remain in keeping with the expectations of the solicitation.
- Vendor assigned staff as presented in the original proposal (individuals and skill sets pledged)

The length of the contract, specifically the contract start date, is dependent upon receiving properly executed award paperwork from the vendor. If award paperwork is received late, the full contract length may be less than indicated above. The contract end date shall remain the same for all vendors. No agreements for services may be executed after the Contract has expired.

1.9 Estimated Value of the Contract

The estimated value of purchase(s) resulting from this Bid is $3.25 million over the life of the potential award, including renewals. MassDOT may add additional funding during the term of the contract.

MassDOT makes no guarantee that any commodities or services will be purchased from any contract resulting from this Bid. Any estimates or past procurement volumes referenced in this Bid are included only for the convenience of Bidders, and are not to be relied upon as any indication of future purchase levels. The estimated value is based on spending on previous, similar contracts.

2 ESTIMATED PROCUREMENT CALENDAR

EVENT	DATE
World Trade Organization (WTO) Notice Posted	5 March 2020
RFR Release Date	XXX
Deadline for Submission of Bid Response Form	Rolling Enrollment – Responses may be submitted ***at anytime***
Notification of Apparent Successful Bidder(s), if any	ongoing
Estimated Contract Start Date	ongoing

Times are Eastern Standard/Daylight Savings (US), as displayed on the COMMBUYS system clock displayed to Bidders after logging in. If there is a conflict between the dates in this Estimated Procurement Calendar and dates in the Bid's Header, the dates in the Bid's Header on COMMBUYS shall prevail. Bidders are responsible for checking the Bid record, including Bid Q&A, on COMMBUYS for Estimated Procurement Calendar updates.

2.1 Amendment Deadline

MassDOT reserves the right to amendment this solicitation after initial publication. It is each interested vendor's responsibility to check COMMBUYS for any amendments, addenda or modifications to this solicitation, and any related solicitation Q&A records. MassDOT accepts no responsibility and will provide no accommodation to Bidders who submit a response based on out-of-date posted information or on information received from a source other than COMMBUYS.

3 SPECIFICATIONS

3.1 Project Goal

MassDOT operates a wide array of transportation systems throughout the Commonwealth, many of which are integrated with Federal and neighboring states. Key Telecommunications, ITS, IPCS Systems are in place to keep these systems running efficiently, providing a safe system for all users. MassDOT seeks to place pre-qualified vendors under Master Service Agreement contracts to supply equipment, parts, and services for the systems in place as well as replacement systems potentially needed in future years, within the terms of this solicitation.

Two primary categories of needs are addressed by this solicitation:

Category 1: Equipment needs and services 43-20-0000

Equipment Purchases
Replacement parts for existing or specialized equipment
Equipment Upgrades
Operating Supplies
Maintenance and/or repair of equipment
Telecommunications/ITS/IPCS equipment parts for Telecommunications, ITS and IPCS Systems
Telecommunications/ITS/IPCS operational and specialized consumables

MassDOT seeks proposals providing anticipated hourly rates on services, maintenance and repair of equipment including percentage discounts from list price for equipment and parts, etc. Further, respondents must be aware that MassDOT requires service at all hours.

Category 2: Consulting and Design Services 81-16-1700

Telecommunications Engineering and Consulting Services
ITS Engineering and Consulting Services
IPCS Engineering and Consulting Services

An indicative list of equipment and systems in place include AFC, PLC, CO, Hydrocarbon, Access Control, Har, two-way radio, RTU, DWDM, fiber optic, Telephony, Traffic/Security CCTV, Ventilation, Automated Gate/Barrier Systems.

MassDOT reserves the right to request that the vendor provide additional related services or products during the term of any contract awarded under this RFR.

In providing services required by this RFR, the successful Bidder will be prepared to support the Commonwealth's conversion to a mile-based exit numbering system on its highways.

Prior to a contract award for this RFR, vendors may be required to present evidence to MassDOT that they have the necessary equipment, storage facilities, experience, ability, and capital to furnish the required materials in the manner prescribed and to perform the required work satisfactorily. ***Response time off-hours is expected to be accelerated and within 24 hours for emergency work. Pricing will be reviewed and approved by the Engineer based on the specifics of theemergency request.***

3.2 Funding of Contract

MassDOT is seeking proposals that demonstrate the best value for equipment, parts, and/or service purchased. Funding may come from a variety of budget sources.

3.3 Confidentiality and Security of Data

The Bidder may work with highly confidential information, sensitive security information, and other information protected from unauthorized disclosure. The Bidder and staff associated with the Contract will abide by MassDOT and other agency confidentiality and privacy provisions, all confidentiality provisions contained in the Contract Terms and Conditions, and all applicable state and Federal laws and regulations, now in effect, or which become effective during the terms of this contract.

3.3.1 Pricing

Vendor selection will include a consideration for product and/or service price. MassDOT will evaluate a percentage discount from list price as part of the pre-qualification process.

MassDOT reserves the right to negotiate price adjustments with any vendor during the term of the Master Service Agreement contract for reasons associated with circumstances beyond the control of the vendor. Proposals must be received 45 calendar days prior to the contract anniversary or extension date. The vendor must submit a formal written request on letterhead for any such adjustment to the MassDOT contract manager.

Proposals for price adjustments must include, but are not limited to:

- Identified price increase and their source, e.g., raw material, freight fuel labor.
- Copies of business publication(s), market quotations, or the trade journals generally recognized-as representative of the trade or industry that indicate market trends for the Contract Commodities.
- Copies of old and new price lists, if applicable, reflecting price changes.

The requested price adjustment(s) must contain a requested effective date. In the event that MassDOT rejects the price change, the Contractor may continue to perform under the extension option.

MassDOT reserves the right to negotiate price and product specifications at any time during the contract period for the best interests of MassDOT. MassDOT reserves the right to request additional information. MassDOT reserves the right to reject any requested price increases which they deem excessive. MassDOT also reserves the right to negotiate decreases in pricing.

3.4 Payment

All payments under this Agreement shall be made in accordance with the Commonwealth's bill paying policy as defined in the Terms and Conditions.

3.5 Subcontracts

Prior written approval from MassDOT is required for any subcontracted services required to meet the objectives of any Statement of Work for services issued under a Master Service Agreement issued as a result of this RFR. Contractors are responsible for the satisfactory performance and

adequate oversight of their subcontractors. MassDOT will hold the vendor responsible for meeting the requirements of the contract even if a subcontractor is performing specific services.

All proposed subcontractors must be disclosed in full. The information furnished must include a description of the work to be performed by each subcontractor and the percentage of the total effort that work represents.

Vendors are responsible for the compliance of its subcontractors and suppliers with all requirements arising under Federal, State and Municipal laws, ordinances, rules and regulations, as may be applicable.

Any consent to subcontract any part of the work shall not be construed to be an acceptance by MassDOT of the subcontract or any of its terms, but shall operate only as authorization to enter into the subcontract between the Bidder and the proposed subcontractor.

3.6 Bidder's Liability

The Bidder hereby agrees to release MassDOT from all liability in connection with the payment of damages, claims, freight charges, demurrage, cost of material and other claims or demands of whatever nature which may arise, during the Contractor's performance of work under any order issued pursuant to a contract awarded under this Request for Response.

The Bidder agrees that title, ownership and the incidents thereto of all materials to be purchased under any contract resulting from this solicitation shall not vest in MassDOT until such materials are delivered and accepted.

3.7 Contract Management (Service Provider's interface with MassDOT's Contract Manager)

Respondents shall provide a Vendor Account Manager. The Vendor Account Manager shall be responsible for oversight and management of contract performance and shall act as the contact person for receipt of notice and other communications between MassDOT and the Contractor. The Vendor Account Manager must respond within 24 hours to MassDOT if contacted.

Vendor Account Manager:

Respondents must provide in its submission the name of at least one individual who will be the Vendor Account Manager. This individual will be responsible for:

- Proper operation and administration of the contract by the vendor.
- Responding in a timely manner and in writing unless instructed otherwise, to all requests from the MassDOT Contract Manager.
- Supplying information and serving as liaison between the vendor and MassDOT.

MassDOT may require the vendor to relieve the Vendor Account Manager if:

- The Account Manager does not support the contract requirements.
- The Account Manager does not deliver work which conforms to the requirements demonstrated in this contract.
- Issues with the Account Manager that hinders effective functioning of the contract.

3.8 Vendor Warranty

Vendors shall honor all manufacturer warranties on materials purchases (equipment, parts, etc), providing for return free of any and all shipping/postage costs and free of the cost of shipping/delivery of any replacement item.

Service on MassDOT equipment shall be warrantied for a minimum of sixty (60) days. There will be no payments made for call-backs for the same issue within the 60 day period, unless manufacture's defect is demonstrated. In such cases, the item shall be replaced at no additional cost by the vendor per the terms of the manufacturer's warranty.

4 AUDIT

During the term of this Agreement and for a period of six (6) years thereafter, MassDOT, its auditors, the Office of the Inspector General or other authorized representatives shall be afforded access at reasonable times to selected vendor's accounting records, including sales information on any system, reports or files, in order to audit all records relating to goods sold or services performed pursuant to this Agreement. If such an audit indicates that the selected vendor has underperformed in providing goods or services to MassDOT, then the vendor shall remit the funds due and be responsible for payment of any costs associated with the audit.

5 EVALUATION CRITERIA

A Selection Committee comprised of employees from MassDOT and its subject matter experts will use the following process and criteria to evaluate proposals and select vendors based on overall best value:

Evaluation criteria include:

For parts and equipment

- Price - percent discount from list/catalogue

For service:

- Hourly rates
- Accessibility to facilities throughout the Commonwealth

For all

- Nature of business is consistent with the goals and needs of MassDOT
- Experience - Years in Business
- Proven experience/qualifications of the Vendor Account Manager
- Business References (Minimum of three relevant references required) [2]
- Prompt Payment Discount
- Supplier Diversity Commitment

The Selection Committee must be able to determine that the Bidder has the management, technical experience and capacity, and capabilities to perform the requirements of the scope of services. Failure to provide the information necessary to meet these requirements in their response may result in disqualification.

While price will be heavily valued in the evaluation criteria, MassDOT seeks best overall value. Awards will be made to the responsible Bidder whose proposal is most advantageous to MassDOT, but not necessarily to any particular vendor quoting the lowest dollar amount or lowest rates. MassDOT reserves the right to request clarification of responses following submission, and to determine that any non-compliance is insubstantial, can be corrected, or that an alternative proposed by the respondent is acceptable.

6 BID QUALIFICATIONS

MassDOT reserves the right to suspend, withdraw, or amend this RFR at any time, for any reason, and to reject any Proposal not submitted in conformance with the requirements of this solicitation. This RFR is not an offer, and it is not being issued by MassDOT under any statutory requirement.

Any response submitted in response to this RFR may be rejected if in MassDOT's sole judgment it fails to meet the requirements of the RFR, is incomplete, conditional, or obscure; contains additions, deletions, alterations, errors, or other irregularities; or is submitted by a vendor not experienced or capable of performing the scope of services or providing the items sought. MassDOT reserves the right to accept or reject any or all responses.

The successful Bidder must adhere to all Commonwealth and or Federal statutes, regulations, standards and policies related to data privacy and security breaches now in effect or implemented throughout the term of any contract entered into under this RFQ, including without limitation the policies listed hereunder:

EOTSS Security Policies and Standards

https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards

[2] MassDOT may be cited as a reference

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH
http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

EXECUTIVE ORDER NO. 504 ORDER REGARDING THE SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION
]http://www.mass.gov/courts/docs/lawlib/eo500-599/eo504.pdf

Massachusetts General Law 93H Security Breaches
https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H
Payment Card Industry (PCI) Data Security Standard – Version 3.2, or later if applicable
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
Payment Application Data Security Standard – Version 3.2, if applicable
https://www.pcisecuritystandards.org/documents/PA-DSS_v3.pdf
ITD Protection of Sensitive Information - Protection of Personal Data and Information
http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-access-control-policy.html#

Other Terms and Conditions:

Accessibility: The successful Bidder shall comply with the accessibility requirements set forth below (see Accessibility Obligations for Bidders).

Cloud Procurement Terms: The successful Bidder shall comply with the Cloud Terms set forth below (see Cloud Procurement Terms below)

7 FORMS

The following items shall be submitted by Bidder as part of its proposal (also posted separately on COMMBUYS in connection with this RFR):

1. Telecomm Response Form
2. Authorized Signatory Listing Form
3. Executive Order 515, establishing an environmental purchasing policy/EPP plan
4. SDP Plan Form #1 – SDP Plan Commitment
5. Evidence that the vendor is listed under the Commonwealth of Massachusetts Secretary of State's website as licensed to do business in Massachusetts
6. Certificate of Insurance

The following items will form part of any contract entered into with a successful Bidder (posted separately on COMMBUYS in connection with this RFR):

i. MassDOT Standard Contract Form
ii. MassDOT Terms and Conditions
iii. Prompt Pay Discount Form
iv. Massachusetts Substitute W9 Form
v. Electronic Funds Transfer Form
vi. SDP Plan Form #2 – Declaration of SDP Partners

7.1 Supplier Diversity Program

Massachusetts Executive Order 565 reaffirmed and expanded the Commonwealth's policy to promote the award of state contracts in a manner that develops and strengthens certified Minority Business Enterprises (MBEs), Women Business Enterprises (WBEs), Minority and Women Nonprofit Organizations (M/WNPOs), Veteran Business Enterprises (VBEs), Service-Disabled Veteran-Owned Business Enterprises (SDVOBEs), Disability-Owned Business Enterprises (DOBEs), and Lesbian, Gay, Bisexual and Transgender Business Enterprises (LGBTBEs).

Partnerships with M/WBEs, M/WNPOs, VBEs and SDVOBEs: All bidders are **required** to make a significant financial commitment to partner with certified M/WBEs, M/WNPOs, VBEs and/or SDVOBEs certified or verified by the Supplier Diversity Office (SDO). Bidders must identify a commitment in the form of a specific percentage of sales made under the resulting contract that will be spent with an SDP Partner(s) on a Massachusetts fiscal year basis, using SDP Plan Form #1 – SDP Plan Commitment. This percentage commitment will extend for the life of any resulting contract.

This requirement extends to all bidders regardless of their certification status, and no bidder will be awarded a Contract unless and until the above requirement is met. Bidders may not list themselves or affiliates as SDP Partners. In order to ensure compliance with this section and encourage bidder participation, SDP Plans will be evaluated at 10% or more of the total evaluation score for all for Large Procurements (those with a total value of greater than $150,000). SDP Plan submission is encouraged but not required for Small Procurements (those with a total value equal to or less than $150,000).

Once an SDP commitment is approved, the agency will monitor the Contractor's performance, and use the Contractor's reported expenditures with M/WBEs, M/WNPOs, VBEs and SDVOBEs to fulfill their own SDP expenditure benchmarks. The Commonwealth reserves the right to contact SDP Partners at any time to request that they attest to the amounts reported to have been paid to them by the Contractor.

SDP Forms: Unless otherwise specified in the RFR, the following SDP forms are required to be submitted by the deadlines noted below in order to meet the mandatory participation requirements of the SDP:

SDP Plan Form #/Name	Submitted By	When Submitted
SDP Plan Form #1 – SDP Plan Commitment	All Bidders	With Bid Response
SDP Plan Form #2 – Declaration of SDP Partners	Newly Awarded Contractors	Within 30 days of contract execution
SDP Plan Form #3 – SDP Spending Report	Contractors	Within 45 days of the end of each quarter

During the life of the contract, the Commonwealth reserves the right to expand the range of certified business categories available for SDP partnerships to all those mentioned above and/or request reports on the Contractors' spending with such certified business categories.

Supplier Diversity Program (SDP) Resources:

- Lists of M/WBEs, M/WNPOs, VBEs, SDVOBEs, DOBEs and LGBTBEs certified or verified by the Supplier Diversity Office (SDO) are located at www.mass.gov/sdo.
- Resources to assist Prime Bidders in finding potential Certified Partners can be found at www.mass.gov/sdp.
- The Operational Services Division offers trainings on compliance with the SDP Plan requirements. Registration information for upcoming trainings can be found on the Supplier Diversity Program Trainings webpage.

8 HOW TO SUBMIT A RESPONSE

Interested vendors must submit their responses electronically using COMMBUYS. All records on COMMBUYS are comprised of multiple tabs, or pages. Each tab contains data and/or file attachments. All are incorporated into the Bid.

Useful links:

- Job aid on how to submit a quote: https://www.mass.gov/files/documents/2019/03/19/Create-Quote-In-COMMBUYS.pdf
- Webcast: How to Locate and Respond to a Bid in COMMBUYS, which will familiarize Bidders with COMMBUYS terminology, basic navigation, and provide guidance for locating bid opportunities in COMMBUYS and submitting an online quote.
- Bidder may contact the COMMBUYS Help Desk at COMMBUYS@state.ma.us or call during normal business hours (8AM – 5PM, Monday – Friday except on federal, state and Suffolk County holidays) at 1-888-MA-STATE.
- It is each vendor's responsibility to check COMMBUYS for:
    - Any addenda or modifications, by monitoring the Amendment tab, and
    - Any other records related to this Bid.

MassDOT accepts no responsibility and will provide no accommodation to vendors who submit a response based on an out-of-date Bid or on information received from a source other than COMMBUYS.

9 REQUIRED TERMS

9.1.1 Alterations

Vendors may not alter (manually or electronically) the RFR language or any solicitation component files, except as directed in this RFR. Modifications to the body of the RFR, specifications, terms and conditions, or which change the intent of this RFR are prohibited and may disqualify a response.

9.1.2 Ownership of Submitted Quotes

MassDOT shall be under no obligation to return any response or materials submitted by a vendor in response to this solicitation. All materials submitted by vendors become the property of MassDOT and will not be returned. MassDOT reserves the right to use any ideas, concepts, or configurations that are presented in a response, whether or not the response/vendor is selected for Contract award.

9.1.3 Prohibitions

Vendors are prohibited from communicating directly with any employee of MassDOT regarding this RFR except as specified in this RFR, and no other individual MassDOT employee or representative is authorized to provide any information or respond to any question or inquiry concerning this RFR. Vendors may contact the contact person using the information provided on the Header Information this solicitation in the event that this RFR is incomplete or information is missing. Vendors experiencing technical problems accessing information or attachments stored on COMMBUYS should contact the COMMBUYS Helpdesk (see the document cover page for contact information).

In addition to the certifications found in the MassDOT's Standard Contract Form, by submitting a response, the vendor certifies that any response or quote has been arrived at independently and has been submitted without any communication, collaboration, or without any agreement,

understanding or planned common course or action with, any other vendor/supplier of the commodities and/or services described herein.

9.2 Terms and Requirements Pertaining to Awarded Contracts

9.2.1 Commonwealth Tax Exemption

Invoices or invoices submitted to Massachusetts government entities must not include sales tax.

9.2.2 Vendor Contact Information

It is the vendor's responsibility of the to keep current the email address of the Bidder's contact person and prospective contract manager, if awarded a contract, and to monitor that email inbox for communications from MassDOT, including requests for clarification.

MassDOT assumes no responsibility if a prospective vendor's designated email address is not current, or if technical problems, including those with the vendor's computer, network or internet service provider (ISP), cause e-mail communications between the Bidder and MassDOT to be lost or rejected by any means including email or spam filtering.

9.2.3 Publicity

Any vendor awarded a contract under this RFR is prohibited from selling or distributing any information collected or derived from the contract or resultant purchase order, including lists of participating Eligible Entities, MassDOT employee names, telephone numbers or addresses, or any other information except as specifically authorized by MassDOT.

9.2.4 Standards of Performance and Qualifications

Each responding vendor affirms that it is qualified and shall at all times remain qualified to perform as anticipated by the stated goals/objectives of this solicitation. The performance shall be timely and meet or exceed industry standards for the performance required, and vendors shall obtain and maintain all requisite licenses, registrations, permits and resources for performance. Vendors further agree that all services provided will conform to the professional industry standards of care and practice customarily provided by comparable firms engaged in performing comparable services. The personnel furnishing the services will be qualified and competent to perform the services assigned to them. The recommendations, guidance and performance of these personnel will meet such standards of knowledge, judgment and care. Vendors further agree that the services will be free from errors that are the result of the Bidder's negligent failure to conform to those standards.

Each responding vendor must certify that it is listed under the Commonwealth of Massachusetts Secretary of State's website as licensed to do business in Massachusetts, as required by law.

10 INSURANCE

Bidders shall certify on letterhead their understanding and agreement that during the term of any contract arising out of this RFR, the successful Bidder shall continually maintain, with insurance carriers licensed to do business in the Commonwealth of Massachusetts:

i. Commercial General Liability insurance with limits at least equal to One Million Dollars ($1,000,000.00) per occurrence for bodily injury and property damage, One Million Dollars ($1,000,000.00) for personal injury and Two Million Dollars ($2,000,000.00) in the general aggregate. Coverage shall also include limits at least equal to Two Million Dollars ($2,000,000.00) for products and completed operations. All Commercial General Liability coverage shall continue for seven (7) years following completion of the contract. Coverage shall be equivalent to ISO Form CG 01 01 12 07. Coverage shall be provided on a first dollar basis without a deductible. Any Commercial General Liability policy subject to a deductible must be approved in writing in advance by MassDOT;

ii. Automobile Liability insurance with limits at least equal to One Million Dollars ($1,000,000.00) per accident, bodily injury and property damage combined. Coverage shall include non-owned and hired liability;

iii. Workers' Compensation insurance as follows:
   1) Coverage A Workers' Compensation: Statutory as required by Massachusetts law.

   2) Coverage B Employer's Liability: (i) bodily injury by accident One Million Dollars ($1,000,000.00) each accident, (ii) bodily injury by disease One Million Dollars ($1,000,000.00) each employee and (iii) bodily injury by disease One Million Dollars ($1,000,000.00) policy limit; and

iv. Umbrella insurance with limits at least equal to Ten Million Dollars ($10,000,000.00) per occurrence and Ten Million Dollars ($10,000,000.00) in the aggregate. Self-insured retention shall not exceed Ten Thousand Dollars ($10,000.00). Coverage shall be equivalent or broader than the coverage afforded on the underlying Commercial General Liability, Automobile Liability and Employer's Liability grant within the Workers' Compensation policy.

v. Errors and Omissions Liability Insurance with limits of not less than twice the value of the contract in aggregate for the period beginning with the effective date of the contract and ending on the date of final acceptance or the end of the warranty period whichever occurs later. The policy must include an endorsement that provides a discovery period of three (3)

years following the date of final acceptance, and its coverage must extend to and include liability for infringement of intellectual property rights, development and implementation of software that enables access to data over the Internet and the warranty obligations.

All policies shall have a minimum AM Best Rating of A. All policies shall contain a waiver of subrogation in favor of MassDOT and the Workers' Compensation policy shall be specifically endorsed to provide such waiver.

The successful Bidder shall provide certificates of insurance evidencing the foregoing coverage prior to the commencement of performance. The successful Bidder shall, through the term of the contract, provide to MassDOT certificates of insurance evidencing renewal and continuation of this insurance prior to the expiration of any policy. Each insurer will provide notification to MassDOT in writing thirty (30) days in advance of the cancellation, non-renewal, or material change in coverage of the policy.

The successful Bidder shall cause its subcontractors to purchase, carry, and maintain all insurance coverage and coverage limits that this RFR requires the successful Bidder to have.

The cost of the insurance that the successful Bidder and its subcontractors are required to purchase, carry, and maintain is an item that is included in the fixed proposal price.

11 OTHER SPECIFICATIONS

Issue Date: November 1, 2005
Refresh Date: June 6, 2016

The following RFR provisions appear in this section at the department's discretion. If a specification is selected by the department, it is required of the bidder.

Access to Security-Sensitive Information. This solicitation contains security-sensitive information which, pursuant to MGL c. 4, s. 7, cls. 26(n), is generally exempt from public disclosure under the Commonwealth's public records laws and must, for public safety purposes, be safeguarded from widespread public disclosure. This security-sensitive information is in the form of blueprints, plans, policies, procedures, schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, and/or any other records relating to the security or safety of persons (pursuant to M.G.L. c. 66A) or buildings, structures, facilities, utilities, transportation, information technology or other infrastructure located within the commonwealth.

Qualified prospective bidders that are interested in accessing this information for the purpose of preparing a bid response must, before being allowed to access the information, sign a confidentiality agreement, thereby agreeing to:

1. restrict the use of these sensitive records for any other purpose than as authorized and for the purpose of putting together a bid proposal;
2. safeguard the information while it is in their possession (consistent with Section 6 of the *Commonwealth Terms and Conditions*); and
3. return such records and materials to the Commonwealth upon completion of the project.

Alternatives. A response which fails to meet any material term or condition of the RFR, including the submission of required attachments, may lose points or be deemed unresponsive and disqualified. Unless otherwise specified, bidders may submit responses proposing alternatives which provide equivalent, better or more cost effective performance than achievable under the stated RFR specifications. These alternatives may include related commodities or services that may be available to enhance performance during the period of the contract. The response should describe how any alternative achieves substantially equivalent or better performance to that of the RFR specifications.

The department will determine if a proposed alternative method of performance achieves substantially equivalent or better performance. The goal of this RFR is to provide the best value of commodities and services to achieve the procurement goals of the department. Bidders that propose discounts, uncharged commodities and services or other benefits in addition to the RFR specifications may receive a preference or additional points under this RFR as specified.

Contractors may also propose alternatives for equivalent, better or more cost effective performance than specified under the contractor's original response to enable the department to take advantage of enhanced technologies, commodities or services which become available during the term of the contract.

Brand Name or Equal. Unless otherwise specified in this RFR, any reference to a particular trademark, trade name, patent, design, type, specification, producer or supplier is not intended to restrict this RFR to any manufacturer or proprietor or to constitute an endorsement of any commodity or service, and the department may consider clearly identified offers of substantially equivalent commodities and services submitted in response to such reference.

Debriefing. *(This specification is at the department's discretion for non-POS RFRs.)* Non-successful bidders may request a debriefing from the department. Department debriefing procedures may be found in the RFR. "POS" refers to Purchase of Service (POS) human and social services procured under *801 CMR 21.00, Procurement of Commodities or Services, Including Human and Social Services* and *808 CMR 1.00, Compliance, Auditing and Reporting and for Human and Social Services.*

Emergency Standby Commodities and/or Services. Due to a declaration of a state of emergency where the safety and well-being of Commonwealth citizens are at risk, the Commonwealth of Massachusetts may request specific commodities and/or services from its contractors. Contractors may be called upon to supply and/or deliver to the Commonwealth on a priority basis such commodities and/or services currently under contract.

Such accommodations may be requested from a contractor during an actual emergency. To accommodate such requests, contractors may be requested and must make every effort to service these requests from regular sources of supply at the rates set forth in any standard contract resulting from this RFR.

Environmentally Preferable Products and Services. The department and contractor(s) may negotiate during the contract term to permit the substitution or addition of Environmentally Preferable Products (EPPs) when such products are readily available at a competitive cost and satisfy the department's performance needs.

Estimated Provisions. The Commonwealth makes no guarantee that any commodities or services will be purchased from any contract resulting from this RFR. Any estimates or past procurement volumes referenced in this RFR are included only for the convenience of bidders, and are not to be relied upon as any indication of future purchase levels.

Performance and Payment Time Frames Which Continue Beyond the Duration of the Contract. All term leases, rentals, maintenance or other agreements for services entered into during the duration of this contract and whose performance and payment time frames extend beyond the duration of this contract shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, rentals, maintenance or other

agreements for services may be executed after the contract has expired. Any contract termination or suspension pursuant to this section shall not automatically terminate any leases, rentals, maintenance or other agreements for services already in place unless the department also terminates said leases, rentals, maintenance or other agreements for service, which were executed pursuant to the main contract.

Reverse Auction Participation and Payment. In addition to negotiations and Best and Final Offers (BAFOs) that may be conducted with bidders pursuant to 801 CMR 21.00, the SST will be conducting a Reverse Auction subsequent to the submission of proposals. After the conclusion of the reverse auction and the determination of the winning bidder(s), the winning bidder(s) will be responsible for paying the cost for this reverse auction, not to exceed $3,000 per event, directly to the Commonwealth's reverse auction contractor. That payment must be made within 30 days of the end of the auction event or of the contract award date, whichever is later. In the case of multiple winners, the department will determine how payments will be made in a fair and equitable manner. In addition, the SST reserves the right to employ the use of reverse auctions at any time during the contract term under the same payment terms as referenced above in this section.

12 MASSDOT TELECOMM RESPONSE FORM –

Equipment, Parts & Services for Telecommunications, ITS, IPCS Systems

The following requested information is a requirement of the Request for Response (RFR). Failure to complete all sections of this form may be cause for the bid to be deemed as non-responsive and may result in disqualification.

Once completed, save the file and submit via Commbuys using the following naming protocol: **2020_Telecomm_Response_Company.** ***(Note: Please be neat or type in responses – illegible responses will not be accepted!)***

Item	*Use this column for response*
Company Information Legal Company Name	
Address (Street, City, State, Zip)	
Main Phone Number	
Fax Number	
Massachusetts Vendor Code (if known)	VC
Website	
Number of Years in Business, including the year the business was established	
Contract Account Manager Name	
Direct Dial Number	
Fax Number	
Email	
Brief statement of business type – (parts, service offered)	
Brief statement of experience	

Nature of Business *(check one or both)*	[ ] **Category 1: Equipment needs and services** [ ] **Category 2: Consulting and Design Services**
Price Information	*Use this column for response*
Hourly rates	
Parts: percent discount from list/catalogue	
Delivery Charges	
Service Ability	*Use this column for response or attach a brochure/descriptive list*
Describe the type of equipment for which parts/services are provided	
Describe the specific manufacturers for which parts/equipment are Provided	

All responses must also include the additional forms shown below. Each are available with the solicitation posting on Commbuys.

Business Reference Form (provide at least three relevant business references)
Prompt Payment Discount Form
Supplier Diversity Form 1

These will be considered as part of the evaluation.

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this 28 day of July 2022 by and between the **Department of State Police**, hereinafter referred to as "Department," and the **Attleboro Police Department**, a public entity, hereinafter referred to as "Agency," collectively referred to as "Parties."

WHEREAS, the Department contracts the services of one or more vendors to host an Automated License Plate Recognition (ALPR) database to store ALPR data; and

WHEREAS, the Parties provide public safety services within their respective jurisdictions; and

WHEREAS, the Parties have found it to be of mutual benefit to provide for the most efficient utilization of their resources and services in the application to public safety efforts within their respective jurisdictions; and

WHEREAS, the Parties are committed to cooperation and coordination in providing the highest level of public safety services to the public, guided by the principle that performing cooperatively is in the best interest of the public; and

WHEREAS, the Agency desires to use the ALPR system contracted and managed by the Department to facilitate the storage of ALPR information generated by the Agency; and

WHEREAS, the Agency desires to share law enforcement information owned by the Agency under the conditions set forth in this Agreement.

NOW, THEREFORE, for and in consideration of the covenants contained herein, IT IS HEREBY AGREED, by and between the Parties as follows:

1. PURPOSE:

The purpose of this Agreement is to provide a standardized approach and method of storage, retention, sharing, and access of ALPR data between the Department and Public Safety Agencies hosting ALPR data on the Department's ALPR system.

2. COSTS:

The Department shall be responsible for the costs of purchasing and maintaining the ALPR system as long as such funding is available to the Department and authorized by the appropriate authorities of the Commonwealth. Participating agencies shall be responsible for the costs of purchasing, servicing, maintaining, repairing, and/or licensing the ALPR equipment used by their respective agency. The Department shall not be responsible for any costs incurred by the Agency for the purchasing, servicing, maintaining, repairing, and/or licensing of the ALPR equipment owned or used by the Agency. The Agency shall inspect the Agency's ALPR equipment on a regular basis and document each inspection. Any irregularities or malfunctions of any ALPR equipment owned by the Agency or of any ALPR information shall be reported to the Department immediately and shall be addressed and repaired by the Agency as soon as reasonably possible.

3. DATA ACCESS AND SECURITY REQUIREMENTS:

a. System Availability: The Department will work with the vendor(s) to keep the ALPR system software and servers online and available with downtime limited to necessary system maintenance activities or to any outages that are beyond the control of the Department.

b. Data Sharing: ALPR data contributed by the Agency will be accessible for official purposes to all Agencies that have entered into an ALPR Agreement with the Department. The Agency shall not otherwise share ALPR data with or provide ALPR data to any person, entity, or government agency, other than a law enforcement agency, unless such disclosure is authorized by policy or court order or unless such disclosure is required by the Massachusetts Rules of Criminal Procedure or Rules of Superior Court governing discovery in criminal matters.

c. Security Requirements: The Department and the Agency agree to enforce and maintain security requirements for the information stored in the ALPR system as specified in the Agreement. The Agency agrees that the information hosted in the ALPR system shall be used for law enforcement purposes only and that only law enforcement agency employees that have been subject to appropriate background screening shall be allowed access to the system.

   Background screenings must be fingerprint-based and include check of both the state and national criminal history repositories. If a felony conviction of any kind is found, access to ALPR system shall not be granted. The Agency agrees not to share passwords, user logins, or allow the ALPR software to be otherwise used by Agencies who have not entered into an Agreement with the Department allowing such activity.

An employee of the Agency may operate an ALPR unit that is connected to the Department's ALPR system or access the Department's ALPR system software only if the person has been designated as an authorized user by the Chief of the Agency or designee, and has received training from the Agency or the Department on the proper use and operation of ALPRs and any policy or procedures governing the use of ALPRs and ALPR data issued or adopted by the Agency.

4. IMPLEMENTATION OF POLICY:

The Agency shall, within 30 days of execution of this Agreement, adopt the Department's General Order TRF-11 as the policy and procedure document that will govern the Agency's use of and interaction with the Department's ALPR system. The Agency agrees that it has been provided with physical or electronic copy of General Order TRF-11, has had sufficient time to read, review, and understand the document in its entirety, and agrees to be bound by the provisions contained therein. The Department agrees to inform the Agency of any updates or modifications to General Order TRF-11, and the Agency understands and agrees that any updates to General Order TRF-11 will be binding upon the Agency unless the Agency elects to terminate the Agreement and withdraw from participation in the Department's ALPR system.

5. BENEFITS TO AGENCY:

a. Data Links: The centralized storage of ALPR data will provide a solution to the problem of inaccessible or irretrievable information due to disconnected ALPR systems and the difficulty in sharing information across jurisdictional boundaries.

b. Reduction of Costs: The centralized storage of ALPR data will reduce the financial burden to the Agency that is associated with purchasing and maintaining ALPR software.

6. RECORDS AND REPORTS:

The Department protects all ALPR information as personally identifiable information (PII) because ALPR information may be combined with other information to specifically identify a unique individual. As such, all information retained in the Department's ALPR system is the sole property of the Department. The Agency agrees that information stored in the ALPR system for the Agency may be subject to disclosure under certain circumstances. The Agency will refer to the Department for review all information requests for Agency information, including, but not limited to, public records requests, court orders, legal motions, subpoenas, and/or summonses. The Department's Legal Department shall determine the best manner of responding to all requests for Agency information.

7. RETENTION

All ALPR information obtained by the Agency from the Department's ALPR system shall be retained pursuant to the Department's General Order TRF-11.

8. AMENDMENTS:

Any changes and additions to this Agreement shall be made by written amendments to this Agreement and shall not be effective until approved in writing by the Parties. A joint review of this Agreement may be requested at any time by either of the Parties to identify needed changes, which may be amended by written mutual agreement of the Parties.

9. DURABILITY:

This Agreement shall become operational and effective upon execution by the Parties. Parties may terminate the Agreement at any time by giving written notice to the other Parties at least thirty (30) days prior to the effective date of termination. The Agreement may also be terminated by the Department without prior notice to the Agency in the event of executive, legislative, or judicial mandate which requires the unanticipated discontinuation or modification of the ALPR program. In the event of such termination, the Department will notify the Agency as soon as practicable.

10. BENEFITS:

The Parties shall agree that the provisions of this Agreement are not intended to directly benefit and shall not be enforceable by any person or entity not a party to this Agreement. This Agreement is not intended to confer any legal rights or benefits on any person or entity other than the Parties of this Agreement.

11. INDEMNIFICATIONS:

Parties shall defend, indemnify, and hold harmless every other party and its officers, agents, employees, and representatives from any and all losses, liability, damages, claims, suits, actions and administrative proceedings, and demands and all expenditures and cost relating to acts or omissions of the indemnitor, its officers, agents, or employees arising out of or incidental to the performance of any of the provisions of this Agreement. Parties do not assume liability for the acts or omissions of persons other than their respective officers, its employees, agents, and MOU officers.

The Agency releases the Department from any liability relating to the loss or destruction of data contributed by the Agency. The Agency further releases the Department from any liability relating to the loss of the Agency's access to the ALPR system due to system outage, commercial vendor failure or malfeasance, or executive, legislative, or judicial mandate which requires the unanticipated discontinuation or modification of the ALPR program. The Agency further releases the Department from any liability relating to the release of data or information contributed by the Agency pursuant to a lawful procedure or order.

12. ASSIGNMENT PROHIBITED:

Parties to this Agreement may not assign any right or obligation pursuant to this Agreement. Any attempted or purported assignment of any right or obligation pursuant to this Agreement shall be void and of no effect.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the date as written below.

	Kyle P. Heagney
Colonel Christopher S. Mason Massachusetts State Police	Representative: Agency:
	July 28, 2022
Date	Date

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lieutenant Governor

State of New Jersey
OFFICE OF THE ATTORNEY GENERAL
DEPARTMENT OF LAW AND PUBLIC SAFETY
PO BOX 080
TRENTON, NJ 08625-0080

PAULA T. DOW
Attorney General

DIRECTIVE NO. 2010-5

TO: Director, Office of Homeland Security and Preparedness
Director, Division of Criminal Justice
Superintendent, New Jersey State Police
All County Prosecutors
All County Sheriffs
All Police Chiefs
All Law Enforcement Chief Executives

FROM: Paula T. Dow, Attorney General

DATE: December 3, 2010

SUBJECT: **Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data**

In order to fulfill the mission of protecting the public, the New Jersey law enforcement community must take full advantage of new crime-fighting technologies as they become available. Automated license plate readers (ALPRs) are now being used by a number of law enforcement agencies around the nation, and a number of police agencies in New Jersey have recently acquired these devices or are planning to do so in the near future. License plate recognition technology can be used to support a wide range of law enforcement operations and activities, including homeland security, criminal and terrorist suspect interdiction, revoked/suspended driver interdiction, stolen property recovery, stay-away order enforcement and, of course, the apprehension of individuals who are subject to an outstanding arrest warrant.

These devices enable police officers to recognize and take immediate action against vehicles and persons who are subject to an investigative detention or arrest based on a "Be on the Lookout" bulletin. The data collected by ALPRs can also provide solid investigative leads if, for example, a device happened to be scanning license plates near a crime scene, allowing police to locate potential suspects, witnesses, or victims by identifying vehicles that were in the vicinity at the time of the

offense. A careful analysis of stored ALPR data can also be used to detect suspicious activities that are consistent with the *modus operandi* of criminals. This new technology can in this way serve an especially important role in protecting our homeland from terrorist attack, as shown by the fact that many of the devices that are now or soon will be in operation in this State were purchased with homeland security grant monies.

While license plate recognition technology can help to protect public safety, the widespread deployment and use of ALPRs, and especially the collection and storage of data pertaining to individuals who are not reasonably believed to be involved in unlawful activity, raise legal and policy issues. Notably, the New Jersey Supreme Court has held that while police are permitted to "run the plates" of any vehicle they encounter while on patrol, and need not have a particularized reason before checking a vehicle's license plates against a government database, police in this State may not as a result of any such lookup be shown personal identifying information about a motorist unless there is a particularized basis for further police action. See State v. Donis, 157 N.J. 44 (1998). The Guidelines attached hereto are designed to protect the legitimate privacy interests of motorists by implementing the non-disclosure rule established in Donis and by adapting the Donis Court's rationale to the context and capabilities of ALPR technology.

Recognizing that our experience with this new and evolving technology is limited, and that we still have much to learn about how best to incorporate these devices into our arsenal of investigative techniques, it is appropriate for me as the State's chief law enforcement officer to issue uniform statewide guidelines to ensure that ALPRs are used only for *bona fide* law enforcement purposes, and that the data collected by these devices are used in accordance with substantive standards and procedural safeguards that appropriately balance the need for law enforcement agencies to prevent and respond to terrorism and other forms of crime against the legitimate privacy interests of persons operating motor vehicles on the roadways of this State.

THEREFORE, I, Paula Dow, Attorney General of the State of New Jersey, pursuant to the authority granted to me by the Constitution of the State of New Jersey and by the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 *et seq.*, and in consultation with the Director of the New Jersey Office of Homeland Security and Preparedness, hereby Direct the following:

1. Adoption of Guidelines

The "*Attorney General Guidelines for the Use of Automated License Plate Readers and Stored ALPR Data*" (dated December 3, 2010) attached to this Directive and incorporated by reference into this Directive are hereby adopted and shall be followed and enforced by all law enforcement agencies and officers operating under

the authority of the laws of the State of New Jersey.

2. Implementation

Every law enforcement agency operating under the authority of the laws of the State of New Jersey that possesses or uses one or more automated license plate readers shall, within 45 days of the issuance of this Directive, promulgate and enforce a rule, regulation, standard operating procedure, directive, or order, in a form as may be appropriate given the customs and practices of the agency, which shall comply with and implement the provisions of the attached Guidelines, and which shall provide that any sworn officer or civilian employee of the agency who knowingly violates the agency's rule, regulation, standard operating procedure, directive, or order shall be subject to discipline. A law enforcement agency operating under the authority of the laws of the State of New Jersey that purchases an automated license plate reader on or after the effective date of this Directive shall not operate the device without having promulgated a rule, regulation, standing operating procedure, directive, or order in accordance with this section.

3. Scope

The provisions of this Directive and of the attached Guidelines pertaining to stored ALPR data apply to all law enforcement agencies operating under the authority of the laws of the State of New Jersey that access or use stored ALPR data, even if the agency does not own or operate an ALPR.

4. Questions and Controversies

All questions concerning the interpretation, implementation, or enforcement of this Directive, or of the attached Guidelines, shall be addressed to the Attorney General or his or her designee.

5. Periodic Review

The Director of the Division of Criminal Justice, in consultation with the Superintendent of the New Jersey State Police, the Director of the Office of Homeland Security, the County Prosecutors, the County Sheriffs, and the New Jersey Association of Chiefs of Police, shall, within one year of the effective date of this

Directive, report to the Attorney General on the implementation of this Directive, and on any recommendations for revising the attached Guidelines.

6. Effective Date

This Directive shall take effect 45 days after it is issued in order to provide an opportunity for law enforcement agencies to comply with its requirements and to establish and enforce policies and procedures consistent with the attached Guidelines. Once effective, this Directive shall remain in force and effect unless and until a repealed, amended, or superseded by Order of the Attorney General.

Paula T. Dow
Attorney General

Attest:
Carolyn Murray
Counsel to the Attorney General

Issued on: December 3, 2010
Effective on : January 18, 2011

ATTORNEY GENERAL GUIDELINES FOR THE USE OF AUTOMATED LICENSE PLATE READERS (ALPRs) AND STORED ALPR DATA

(Issued December 3, 2010; Effective January 18, 2011)

1. PURPOSE AND SCOPE

1.1 Reasons for Promulgating Uniform Statewide Guidelines

The purpose of these Guidelines is to provide direction to law enforcement agencies and officers on the appropriate us e of Automated License Plate Readers (ALPRs) and the data that are collected by these devices and stored for future law enforcement use. These Guidelines are not intended to serve as a comprehensive operational manual. Rather, they are meant to ensure that ALPRs and ALPR-generated data are used in an appropriate manner and only for *bona fide* public safety purposes.

The following Guidelines, which are promulgated pursuant to Attorney General Law Enforcement Directive 2010-5, should be interpreted and applied so as to achieve the following objectives:

- to ensure that "BOLO lists" (the compilation of targeted license plates that an ALPR is "on the lookout" for) that are programmed into the internal memory of an ALPR or that are compared against stored ALPR data are comprised only of license plates that are associated with specific vehicles or persons for which or whom there is a legitimate and documented law enforcement reason to identify and locate, or for which there is a legitimate and documented law enforcement reason to determine the subject vehicle's past location(s) through the analysis of stored ALPR data;

- to ensure that data that are captured by an ALPR can only be accessed by appropriate law enforcement personnel and can only be used for legitimate, specified, and documented law enforcement purposes;

- to permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used as a means to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst; and

- to ensure that stored ALPR data are purged after a reasonable period of time so as to

minimize the potential for misuse or accidental disclosure.

1.2 Applicability of Guidelines

These Guidelines apply to all law enforcement agencies that operate under the authority of the laws of the State of New Jersey that own or operate one or more ALPRs, that collect and maintain ALPR data, and/or that receive or are provided access to ALPR data collected by another agency.

1.3 Non-Enforceability of Rights by Third Parties

These Guidelines are issued pursuant to the Attorney General's authority under the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 *et seq.*, to ensure the uniform and efficient enforcement of the laws. These Guidelines impose limitations on the exercise of law enforcement discretion and the use of and access to ALPR-related data that may extend beyond the requirements of the United States and New Jersey Constitutions, and federal and state statutory law. Nothing in these Guidelines should be construed in any way to create any rights beyond those established under the Constitutions, statutes, and regulations of the United States and the State of New Jersey. The provisions of these Guidelines are intended to be implemented and enforced by law enforcement agencies that possess or use ALPRs, the New Jersey Office of Homeland Security and Preparedness, the County Prosecutors, and the Department of Law and Public Safety, and these provisions do not create any rights that may be enforced by any other persons or entities.

3. DEFINITIONS

As used in these Guidelines:

"Automated License Plate Reader" or "ALPR" means a system consisting of a camera, or cameras, and related equipment that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device, that automatically converts digital photographic images of scanned license plates into electronic text documents, that is capable of comparing scanned license plate text data with data files for vehicles on a BOLO (be on the lookout) list programmed into the device's electronic memory, and that notifies police, whether by an audible alert or by other means, when a scanned license plate matches the license plate on the programmed BOLO list. The term includes both devices that are placed at a stationary location (whether permanently mounted, or portable devices positioned at a stationary location) and mobile devices affixed to a police vehicle and capable of operating while the vehicle is in motion.

"BOLO (Be on the Lookout)" or "BOLO situation" refers to a determination by a law

enforcement agency that there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle, or, in the case of a post-scan BOLO, there is a legitimate and specific reason to ascertain the past location(s) of a particular vehicle.

"BOLO list," sometimes referred to colloquially as a "hot list," is a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists that is programmed into an ALPR so that the device will alert if it captures the image of a license plate that matches a license plate included on the BOLO list. The term also includes a compilation of one or more license plates, or partial license plates, that is compared against stored license plate data that had previously been scanned and collected by an ALPR, including scanned license plate data that is stored in a separate data storage device or system.

"Initial BOLO list" refers to the BOLO list that was programmed into an ALPR at the time that the device was being used to scan license plates in the field.

"Post-Scan BOLO list" refers to a BOLO list that is compared against stored data collected by an ALPR, including scanned license plate data that has been transmitted to another device or data storage system.

"Stored data" refers to all information captured by an ALPR and stored in the device's memory or in a separate data storage device or system. The term includes the recorded image of a scanned license plate and optical character recognition data, a contextual photo (*i.e.*, a photo of the scanned vehicle and/or occupants), global positioning system("GPS") data (when the ALPR is equipped with a GPS receiver) or other location information, and the date and time of the scan. The term applies to both alert data and non-alert data that has been captured and stored by an ALPR or in a separate data storage device or system.

"Alert data" means information captured by an ALPR relating to a license plate that matches the license plate on an initial BOLO list or a post-scan BOLO list.

"Immediate alert" refers to an alert that occurs when a scanned license plate matches the license plate on an initial BOLO list and that is reported to the officer operating the ALPR, by means of an audible alarm or by any other means, at or about the time that the subject vehicle was encountered by the ALPR and its license plate was scanned by the ALPR.

"Non-encounter alert" refers to an immediate alert where the officer operating the ALPR is instructed to notify the agency that put out the BOLO without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention (*e.g.*, a Violent Gang or Terrorist Organization File (VGTOF) alert).

"Personal identifying information" means information that identifies one or more specific individuals, including an individual's name, address, social security number, vehicle operator's

license number, or biometric records. The term includes personal identifying information that is included within the data comprising a BOLO list, as well as personal identifying information that is learned by checking a license plate scanned by an ALPR against the Motor Vehicle Commission database or any other data system that contains personal identifying information.

"Scan" refers to the process by which an ALPR automatically focuses on, photographs, and converts to digital text the license plate of a vehicle that comes within range of the ALPR.

"Authorized user"means a sworn or civilian employee of a law enforcement agency who has been authorized by the chief of the agency, or by the Attorney General or a county prosecutor or his or her designee, to operate an ALPR, or to access and use ALPR stored data, and who has successfully completed training provided by the agency on the agency's ALPR policy and on these Guidelines.

"Designated supervisor" means a superior officer assigned by the chief of a law enforcement agency to oversee and administer, or to assist in overseeing and administering, the agency's use of ALPRs and stored ALPR data. A law enforcement agency may have more than one designated supervisor.

"Chief" of a department or agency means the highest ranking sworn officer of a law enforcement agency.

"Post-Scan BOLO query" refers to the process of comparing a post-scan BOLO list against stored ALPR data.

"Crime scene query" refers to the process of accessing and reviewing stored ALPR data that had been originally scanned at or about the time and in the vicinity of a reported criminal event for the purpose of identifying vehicles or persons that might be associated with that specific criminal event as suspects, witnesses, or victims.

"Criminal event" means a specific incident, or series of related specific incidents, that would constitute an indictable crime under the laws of the State of New Jersey, whether or not the incident(s) have occurred or will occur within the State of New Jersey. The term includes an attempt or conspiracy to commit a crime, or actions taken in preparation for the commission of the crime, such as conducting a surveillance of the location to identify and evade or thwart security measures, or conducting a rehearsal of a planned crime. The term includes two or more separate criminal acts or episodes that are linked by common participants or that are reasonably believed to have been undertaken by a criminal organization or as part of an ongoing conspiracy.

"Crime trend analysis" refers to the analytical process by which stored ALPR data is used, whether alone or in conjunction with other sources of information, to detect crime patterns by studying and linking common elements of recurring crimes; to predict when and where future crimes may occur; and to link specific vehicles to potential criminal or terrorist activity. The term includes

an automated process in which a computer program analyzes stored data to identify potentially suspicious activity or other anomalies involving one or more scanned vehicles and where such automated analysis is done without disclosing personal identifying information about any individual to an authorized user or any other person except as may be authorized pursuant to Section 10.2.3 of these Guidelines.

4. DEPLOYMENT OF ALPRS

4.1 Restricted Uses

An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business.

4.2 ALPR Scanning Limited to Vehicles Exposed to Public View

An ALPR shall only be used to scan license plates of vehicles that are exposed to public view (*e.g.*, vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shopping mall or other business establishment).

4.3 Supervisory Approval of All ALPR Deployments

An ALPR shall not be deployed in the field unless the deployment has been authorized by the chief of the department or a designated supervisor, or by the Attorney General or designee or a county prosecutor or designee. Such authorization may be given for repeated or continuous deployment of an ALPR (*e.g.*, mounting the device on a particular police vehicle, or positioning the ALPR at a specific stationary location), in which event the deployment authorization shall remain in force and effect unless and until rescinded or modified by the chief or designated supervisor, or the Attorney General or county prosecutor or designee.

4.4 Trained Operators and Analysts

A sworn officer or civilian employee of the department may operate an ALPR or access or use ALPR stored data only if the person has been designated as an authorized user by the chief of the department, or by the Attorney General or designee or a county prosecutor or designee, and has received training from the department on the proper use and operation of ALPRs, the requirements of Attorney General Law Enforcement Directive 2010-5, and these Guidelines, and any policies and

procedures governing the use of ALPRs and ALPR data issued by the department pursuant to Attorney General Directive 2010-5and Section 14 of these Guidelines.

5. MAINTENANCE OF RECORDS

5.1 Records Documenting the Deployment of ALPRs

Each department that owns or operates an ALPR shall maintain a written or electronic record that documents the following information:

date and time when the ALPR was deployed;

whether the ALPR was mobile, or was stationed at a fixed specified location;

the identity of the operator;

whether ALPR data was transferred to any other database or data storage device or system.

5.2 Records Documenting the Use of Stored ALPR Data

Each department that stores ALPR data shall maintain a record of all access to stored ALPR data. The department's ALPR data record keeping system, which may be automated, shall document the following information:

the date and time of access, and, in the case of access to stored non-alert data, the type of access authorized by Section 10.2 of these Guidelines (*i.e.*, post-scan BOLO query, crime scene query, or crime trend analysis);

the authorized user who accessed the stored data;

whether an automated software program was used to analyze stored data;

the designated supervisor who reviewed and approved any disclosure of personal identifying information based upon crime trend analysis when such approval is required by Section 10.2.3 of these Guidelines;

the designated supervisor who approved any use of an automated crime trend analysis computer program that would automatically alert and disclose personal identifying

information in accordance with Section 10.2.3;

any other information required to be documented pursuant to Section 10.2 or any other provision of these Guidelines.

5.3 Maintenance of Records

All written or electronic records of ALPR activity and access to ALPR data shall be maintained by the department for a period of five years, and shall be kept in a manner that makes such records readily accessible to any person authorized by these Guidelines to audit the department's use of ALPRs and ALPR-generated data. When a department employs an automated system to record any information that is required to be documented pursuant to these Guidelines, it shall not be necessary for the department to maintain duplicate records of any events or transactions that are documented by the automated record-keeping system.

6. CONTENT AND APPROVAL OF BOLO LISTS

6.1 Criteria for and Examples of Legitimate BOLO Situations

A license plate number or partial license plate number shall not be included in an ALPR initial BOLO list unless there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person or persons who are reasonably believed to be associated with that vehicle. A license plate or partial license plate number shall not be included in a Post-Scan BOLO list unless there is a legitimate and specific law enforcement reason to ascertain the past locations(s) of that particular vehicle, or of any person or persons who are reasonably believed to be associated with that vehicle.

Examples of legitimate and specific reasons include, but are not limited to: persons who are subject to an outstanding arrest warrant; missing persons; AMBER Alerts; stolen vehicles; vehicles that are reasonably believed to be involved in the commission of a crime or disorderly persons offense; vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list; vehicles with expired registrations or other Title 39 violations; persons who are subject to a restraining order or curfew issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements; persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity; and persons who are on any watch list issued by a State or federal agency responsible for homeland security.

6.2 Batch Downloading of BOLO List Data

BOLO list information may be downloaded in batch form from other databases, including but not limited to the National Crime Information Center (NCIC), National Insurance Crime Bureau, United States Department of Homeland Security, and Motor Vehicle Commission database.

6.3 Updates to BOLO Lists

An initial BOLO list may be revised at any time. In the event that an initial BOLO list is constructed, in whole or in part, with sets of data downloaded from another database, so as to account for any changes that may have been made in the data maintained in those other databases, updates to the initial BOLO list shall, in the case of a mobile unit attached to a police vehicle, be made at the start of each shift, and in the case of an ALPR positioned at a stationary location, be made as frequently as is practicable, and on not less than a daily basis. Information concerning any license plate that is referenced in an AMBER Alert activated by the New Jersey State Police shall be added to the initial BOLO list as expeditiously as possible, and shall remain in the initial BOLO list until the AMBER Alert expires or is withdrawn.

6.4 Special Instructions for Immediate Alert Response

When practicable, the reason for placing a vehicle on BOLO list shall be included with the BOLO and shall be disclosed to the officer who will react to an immediate alert. If for any reason an officer reacting to an immediate alert should not initiate an investigative detention (*e.g.*, where the license plate was included in the BOLO list because the department or any other agency wanted to be notified of the location of the subject vehicle without alerting the driver/occupants that they are the subject of law enforcement attention, such as in the case of Violent Gang or Terrorist Organization File (VGTOF) alert), to the extent feasible, the information attached to the license plate on the BOLO list shall be entered in such a way as to cause the ALPR to clearly designate an immediate alert as a "non-encounter" alert, and shall provide specific instructions to the officer as to who to notify of the alert. See Section 7, infra.

7. POLICE ACTIONS IN RESPONSE TO AN IMMEDIATE ALERT

When an officer operating a vehicle equipped with an ALPR receives an immediate alert, the officer shall take such action in response to the alert as is appropriate in the circumstances. An officer alerted to the fact that an observed motor vehicle's license plate is on the BOLO list may be required to make a reasonable effort to confirm that a wanted person is actually in the vehicle before

the officer would have a lawful basis to stop the vehicle. See State v. Parks, 288 N.J. Super. 407 (App. Div. 1996) (police do not have reasonable suspicion to justify a stop based on a computer check that shows that the operator's license of the registered owner of the vehicle is suspended unless the driver generally matches the owner's physical description (*e.g.*, age and gender)).

An officer reacting to an immediate alert shall consult the database to determine the reason why the vehicle had been placed on the BOLO list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency that had put out the BOLO. See Section 6.4, supra.

8. SECURITY OF STORED ALPR DATA

8.1 Physical Security and Limited Access

All ALPR stored data shall be kept in a secure data storage system with access restricted to authorized persons. Access to this stored data shall be limited to the purposes described in Section 10 of these Guidelines.

8.2 Differentiation of Stored Positive Alert Data From Non-Alert Data

Stored ALPR data shall be maintained electronically in such a manner as to distinguish alert data from non-alert data so as to ensure that access to and use of non-alert data and any disclosure of personal identifying information resulting from the analysis of non-alert data occurs only as may be authorized pursuant to section 10.2 of these Guidelines. Positive alert data may, as appropriate, be transferred to the appropriate active investigation file, see also Section 10.1, infra, and may as appropriate be placed into evidence in accordance with the department's evidence or records management procedures.

9. RETENTION PERIOD AND PURGING OF STORED DATA

Each law enforcement agency shall, pursuant to the provisions of Section 14 of these Guidelines, establish and enforce procedures for the retention and purging of stored ALPR data in accordance with this Section. ALPR stored data shall be retained for a period of five years, after which, the data shall be purged from the agency's data storage device or system. A law enforcement agency may purge ALPR data before the expiration of the five-year retention period only if the data has been transferred to the State Police Regional Operations Intelligence Center (R.O.I.C.)or any other system that aggregates and stores data collected by two or more law enforcement agencies in accordance with the provisions of these Guidelines. Any ALPR data transferred to another agency

shall indicate the date on which the data had been collected by the ALPR so that the receiving agency may comply with the five-year retention and purging schedule established in this Section. See also Section 11.1 and 11.2, infra.

10. LIMITATIONS ON ACCESS TO AND USE OF STORED ALPR DATA

10.1 Access to Positive Alert Data

An authorized user may access and use stored ALPR alert data as part of an active investigation or for any other legitimate law enforcement purpose, including but not limited to a post-scan BOLO query, a crime scene query, or crime trend analysis. A record shall be made of the access to the data, which may be an automated record, that documents the date of access, and the identity of the authorized user. An authorized user need not obtain approval from the chief or designated supervisor, or Attorney General or county prosecutor or designee, for each occasion on which he or she accesses and uses stored ALPR data. Once positive alert data has been accessed and transferred to an investigation file, it shall not be necessary thereafter to document further access or use of that data pursuant to these Guidelines.

10.2 Access to Non-Alert Data

Access to and use of stored non-alert ALPR data is limited to the following three purposes: a post-scan BOLO query, a crime-scene query, and crime trend analysis. An authorized user does not need to obtain approval from the chief or a designated supervisor, or Attorney General or county prosecutor or designee, for each occasion on which he or she accesses and uses stored non-alert data pursuant to this Section.

10.2.1 Post-Scan BOLO Query

A law enforcement agency is authorized to compare a post-scan BOLO list against stored ALPR data where the results of the query might reasonably lead to the discovery of evidence or information relevant to any active investigation or ongoing law enforcement operation, or where the subject vehicle might be placed on an active initial BOLO list. (For example, a law enforcement agency may review stored non-alert data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned for the purpose of confirming or dispelling an alibi defense, or to develop lead information for the purpose of locating a specified vehicle or person. A law enforcement agency may also check stored data to determine whether a vehicle that was only recently added to an initial BOLO list had been previously observed in the jurisdiction before it had been placed on an initial BOLO list.)

10.2.2 Crime Scene Query

a. A law enforcement agency is authorized to access and use stored non-alert data where such access might reasonably lead to the discovery of evidence or information relevant to the investigation of a specific criminal event as defined in these Guidelines. Note that if the law enforcement agency has reason to believe that a specific person or vehicle was at or near the location of the specific crime at the time of its commission, non-alert stored data might also be examined under the authority of Section 10.2.1 as part of post-scan BOLO query.

b. A crime scene query may not be conducted to review stored non-alert data based on general crime patterns (*i.e., e.g.*, to identify persons traveling in or around a "high crime area"), but rather is limited to situations involving specific criminal events as that term is defined in these Guidelines.

c. The crime scene query of non-alert stored data shall be limited in scope to stored non-alert data that is reasonably related to the specified criminal event, considering the date, time, location, and nature of the specified criminal event. For example, a crime that reasonably involves extensive planning and possible "rehearsals," such as a terrorist attack, would justify examining stored non-alert data that had been scanned and collected days or even weeks or months before the criminal event, and that may have been scanned at a substantial distance from the site of the crime or intended crime (*e.g.*, at any point along a highway leading to the intended crime site). A spontaneous crime, in contrast, might reasonably justify examination of stored non-alert data that was scanned and collected on or about the time of and in closer physical proximity to the criminal event.

d. The law enforcement agency shall document the specific crime or related crimes constituting the criminal event and the date(s) and location(s) of the specific crime(s).

10.2.3 Crime Trend Analysis

a. A law enforcement agency may access and use stored non-alert data for purposes of conducting crime trend analysis, as that term is defined in these Guidelines, when such access and analysis is approved by a designated supervisor and where such analysis is undertaken to produce analytical products that are intended to assist the agency in the performance of its duties. A designated supervisor may authorize one or more authorized users to conduct a method or methods of crime trend analysis on a repeated or continuous basis, in which event such authorization shall remain in force and effect unless and until modified or rescinded by the supervisor. A designated supervisor may also approve the use of an automated software program to analyze stored data to look for potentially suspicious activity or other anomalies that might be consistent with criminal or terrorist activity.

b. Crime trend analysis of stored non-alert data, whether automated or done manually, shall not result in the disclosure of personal identifying information to an authorized user or any other person unless:

1) the agency can point to specific and articulable facts that warrant further investigation of possible criminal or terrorist activity by the driver or occupants of a specific vehicle *(i.e.*, unusual behavior consistent with the *modus operandi* of terrorists or other criminals), and access to the personal identifying information based on those specific and articulable facts has been approved by a designated supervisor. Such approval may be given by a designated supervisor in advance when the crime trend analysis reveals the existence of specified suspicious circumstances that would warrant further investigation and that would justify disclosure of personal identifying information to the authorized user conducting the analysis under the "specific and articulable facts that warrant further investigation" standard of proof established in this Section. The supervisor shall document any and all specified suspicious circumstances for which disclosure of personal identifying information is pre-approved if those suspicious circumstances are revealed by authorized crime trend analysis. When an automated crime trend analysis computer program is used, specified suspicious circumstances that would warrant further investigation and that would justify disclosure of personal identifying information to an authorized user under this Section may also be pre-approved by a designated supervisor and built into the computer program so that if the program identifies the existence of the pre-determined suspicious circumstances, it will automatically alert the authorized user of the suspicious activity and provide to him or her the relevant personal identifying information in accordance with the "specific and articulable facts that warrant further investigation"standard of proof established in this Section; or

2) Disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.

c. Nothing in this Section shall be construed to prohibit a computer program from accessing and comparing personal identifying information of one or more individuals who are associated with a scanned vehicle as part of the process of analyzing stored non-alert data, provided that such personal identifying information is not disclosed to a person unless the "specific and articulable facts that warrant further investigation" standard is satisfied. The "specific and articulable facts that warrant further investigation" standard set forth in this Section applies only to the crime trend analysis of non-alert data, and nothing in this Section shall be construed to limit disclosure of personal identifying information of a person who is the registered owner of a vehicle that is on an initial or post-scan BOLO list (*i.e.*, alert data).

d. For the purposes of this Section, the "specific and articulable facts that warrant further investigation" standard required for the disclosure of personal identifying based upon crime trend

analysis of stored non-alert data is intended to be comparable to the "specific and articulable facts that warrant heightened caution" standard developed by the New Jersey Supreme Court in State v. Smith, 134 N.J. 599, 616-19 (1994) (establishing the level of individualized suspicion required before an officer may order a passenger to exit a motor vehicle stopped for a traffic violation).

e. The law enforcement agency accessing stored non-alert ALPR data for purposes of conducting crime trend analysis shall document: the nature and purpose of the crime trend analysis; the persons who accessed stored non-alert ALPR data for use in conducting that analysis; and the designated supervisor who approved access to ALPR non-alert data. In any instance where personal identifying information is disclosed based upon crime trend analysis of stored non-alert data, the agency shall document the specific and articulable facts that warrant further investigation and the designated supervisor who reviewed those facts and approved the disclosure of personal identifying information, or who pre-approved disclosure of personal identifying information based upon specified circumstances identified by an automated crime trend analysis computer program, or, where applicable, the fact that access to personal identifying information was authorized by a grand jury subpoena.

11. SHARED LAW ENFORCEMENT ACCESS TO STORED ALPR DATA

11.1 Authorization to Share and Aggregate Data

Any ALPR data that may in conformance with these Guidelines be accessed and used by the law enforcement agency that collected the data may be shared with and provided to any other law enforcement agency. Stored ALPR data may be combined with ALPR data collected by two or more law enforcement agencies (*e.g.*, collection of stored data by the State Police Regional Operations Intelligence Center), provided that such aggregated data shall only be retained, accessed, and used in accordance with the provisions of these Guidelines.

11.2 Record of Shared Access and Responsibilities of the Receiving Agency

When ALPR data is made accessible to or otherwise shared with or transferred to another law enforcement agency, the agency that collected the ALPR data shall document the identity of the other agency and the specific officer(s) or civilian employee(s) of that agency who were provided the information. When the transfer of stored ALPR data is done periodically as part of a system for aggregating data collected by two or more law enforcement agencies (*e.g.*, the scheduled and routine transmittal of data to the State Police Regional Operations Intelligence Center), each agency contributing data to the combined database shall maintain a record of the data transfer, which may be an automated record, and shall have and keep on file a memorandum of understanding or agreement or other memorialization of the arrangement for maintaining and populating a database comprised of stored ALPR data collected by multiple law enforcement agencies. Any agency

provided with access to or use of the ALPR data collected by another agency shall comply with all applicable provisions of these Guidelines concerning stored ALPR data and disclosure of personal identifying information.

13. RELEASE OF ALPR DATA TO NON-LAW ENFORCEMENT PERSONS OR AGENCIES

Stored ALPR data shall be treated as "criminal investigatory records" within the meaning of N.J.S.A. 47:1A-1 *et seq.*, and shall not be shared with or provided to any person, entity, or government agency, other than a law enforcement agency, unless such disclosure is authorized by a subpoena or court order, or unless such disclosure is required by the Rules of Court governing discovery in criminal matters. Any agency receiving a subpoena or court order for the disclosure of ALPR data shall, before complying with the subpoena or court order, provide notice to the County Prosecutor, or to the Division of Criminal Justice in the case of any state-level law enforcement agency.

14. PROMULGATION AND ENFORCEMENT OF DEPARTMENTAL POLICIES

14.1 Required Contents of Departmental Policies

Pursuant to the requirements of Attorney General Law Enforcement Directive 2010-5, every law enforcement agency that possesses or uses an ALPR must promulgate and enforce a rule, regulation, standing operating procedure, directive, or order that establishes a comprehensive policy governing the operation of ALPRs, and governing access to, use, and retention of all stored ALPR data. The ALPR policy promulgated by the department must be consistent with the standards and procedural safeguards established in these Guidelines, and each ALPR policy must include the following provisions:

a. The ALPR policy shall provide that the chief of the department will designate one or more superior officers to oversee and administer the agency's ALPR program. These designated supervisors will be authorized to: provide or oversee the training of all officers and civilian employees who are authorized to operate an ALPR or to access or use ALPR stored data; review and approve requests to access and use stored ALPR data to conduct crime trend analysis and/or to access personal identifying information based upon crime trend analysis; and generally to ensure compliance with the department's ALPR policy and these Guidelines.

b. The ALPR policy shall provide that the chief of the department shall designate all

authorized users, and that no officer or civilian employee will be authorized to operate an ALPR, or to access or use ALPR stored data, unless the officer or civilian employee has received training by the department on the proper operation of these devices, and on the provisions of the department's ALPR policy and these Guidelines.

c. The ALPR policy shall implement and enforce the five-years retention period for ALPR stored data established in Section 9 of these Guidelines, and must provide for the purging of all ALPR stored data at the expiration of the five-year term.

d. The ALPR policy shall provide for the documentation of all ALPR-related activities and decisions that are required to be documented by Section 5 or any other provision of these Guidelines, which may be done by an automated record-keeping system, and shall provide that such records documenting the use of ALPRs and ALPR stored data shall be maintained for 5 years and shall be kept in a place and in a manner as to facilitate a review and audit of the department's ALPR program by the County Prosecutor or by the Attorney General or his or her designee.

e. The ALPR policy shall provide that any sworn officer or civilian employee of the agency who knowingly violates the agency's policy, or these Guidelines, shall be subject to discipline.

f. The ALPR policy shall provide that all significant violations of the agency's policy, or of these Guidelines, including but not limited to all instances involving the unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor, or to the Director of the Division of Criminal Justice in cases involving a state-level agency, upon discovery of the violation. Unless the County Prosecutor or Director elects to conduct or oversee the investigation of the violation, such notification of the violation shall be followed up with a report, approved by the chief of the department, explaining to the County Prosecutor, or to the Director, the circumstances of the violation, and the steps that are being taken to prevent future similar violations.

14.2 Notice of ALPR Policies and Revisions Provided to County Prosecutors or the Division of Criminal Justice

The chief of the department shall provide a copy of the agency's written ALPR policy to the County Prosecutor, or to the Division of Criminal Justice in the case of a state-level agency, at or before the time of promulgation, and shall provide to the County Prosecutor, or to the Division, copies of any amendments or revisions to the agency's ALPR policy at or before the time that such amendments take effect.

15. ALPR PROGRAM ACCOUNTABILITY

15.1 ALPR Program Audits

All ALPR records documenting the use of an ALPR, or access to or use of ALPR stored data, whether kept manually or by means of an automated record-keeping system, shall be subject to review and audit by the County Prosecutor, or by the Attorney General or his or her designee.

15.2 Handling of Complaints

Any complaints about a department's ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor, or to the Director of the Division of Criminal Justice in the case of a State-level agency, for appropriate review and handling. The County Prosecutor, or Director, may conduct an investigation, or may direct the agency that is the subject of the complaint to conduct an investigation and to report back to the County Prosecutor or Director.

16. SANCTIONS FOR NON-COMPLIANCE

If the Attorney General or his or her designee has reason to believe that a law enforcement agency or officer or civilian employee is not complying with or adequately enforcing the provisions of these Guidelines, the Attorney General may temporarily or permanently suspend or revoke the authority of the department, or any officer or civilian employee, to operate an ALPR, or to gain access to or use ALPR stored data. The Attorney General or her designee may initiate disciplinary proceedings, and may take such other actions as the Attorney General in his or her sole discretion deems appropriate to ensure compliance with these Guidelines.

17. AUTHORITY OF ATTORNEY GENERAL TO GRANT EXEMPTIONS OR SPECIAL USE AUTHORIZATIONS

ALPRs, and all ALPR stored data, shall only be used and accessed for the purposes and in the manner authorized by these Guidelines. In recognition of the need to be able to address issues or circumstances that are not contemplated by these Guidelines, the Attorney General or his or her designee may grant an exemption from any provision of these Guidelines, and may authorize the specific use of an ALPR, or the data collected by or derived from an ALPR, that is not expressly authorized by these Guidelines. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by these Guidelines shall be made to the Attorney

General or his or her designee through the Director of the Division of Criminal Justice or his or her designee, who shall make recommendations on whether to grant the agency's specific request for an exemption or special authorization. Such requests shall be made in writing unless the circumstances are exigent, in which event the request by the agency and approval or denial by the Attorney General or his or her designee may be given orally, in which event the circumstances of the request and the approval or denial shall be memorialized in writing as soon thereafter as is practicable.



AIRSHIP PRICING CATALOG

LICENSE-BASED SOFTWARE, HARDWARE & PROFESSIONAL SERVICES

CONTENTS

GENERAL TERMS AND CONDITIONS 3
Disclaimer 3
Validity 3
End User License Agreement 3
AIRSHIP PRODUCT PRICING 4
AIRSHIP ADVANTAGE 5
Airship Gold Support 5
Airship Platinum Support 5
AIRSHIP CAMERA LICENSE(S) 6
AIRSHIP ENTERPRISE MANAGEMENT SYSTEM (EMS) 6
Airship Server 7
EDS 7
AIRSHIP CLIENT PRODUCTS 8
Airship Nexus Client 8
Airship Nexus Video Portal 8
Airship Nexus Mobile 8
AIRSHIP EDGE PRODUCTS 9
Airship Outpost 9
Airship Outpost Mobile 9
PRICING 10
Airship Software Pricing 10
Outpost Appliance Pricing 11
ALPR Stream Pricing 12
ALPR Server Pricing 12
Airship Server Pricing 13
AIRSHIP ADVANTAGE - SUPPORT PRICING 14
Outpost Hardware - Support 14
PROFESSIONAL SERVICES AND TRAINING 15

©2022 Airship Industries

GENERAL TERMS AND CONDITIONS

DISCLAIMER

Airship reserves the right to make adjustments to pricing, Products and Service offerings for reasons including, but not limited to, changing market conditions, Product discontinuation, Product unavailability, manufacturer price changes, supplier price changes and errors in advertisements. All orders are subject to Product availability and the availability of Personnel to perform the Services. Therefore, Seller cannot guarantee that it will be able to fulfill Customer's orders if the order is placed after quote expiration or without first consulting a sales representative prior to submitting a purchase order. If Services are being performed on a time and materials basis, any estimates provided by Seller are for planning purposes only.

VALIDITY

The prices are valid from July 01, 2022, and until further notice. All prices are in USD. All prices are manufacturer's suggested retail price (MSRP), excluding tax/VAT and shipment. Price list revision date: Dec 31, 2021.

END USER LICENSE AGREEMENT

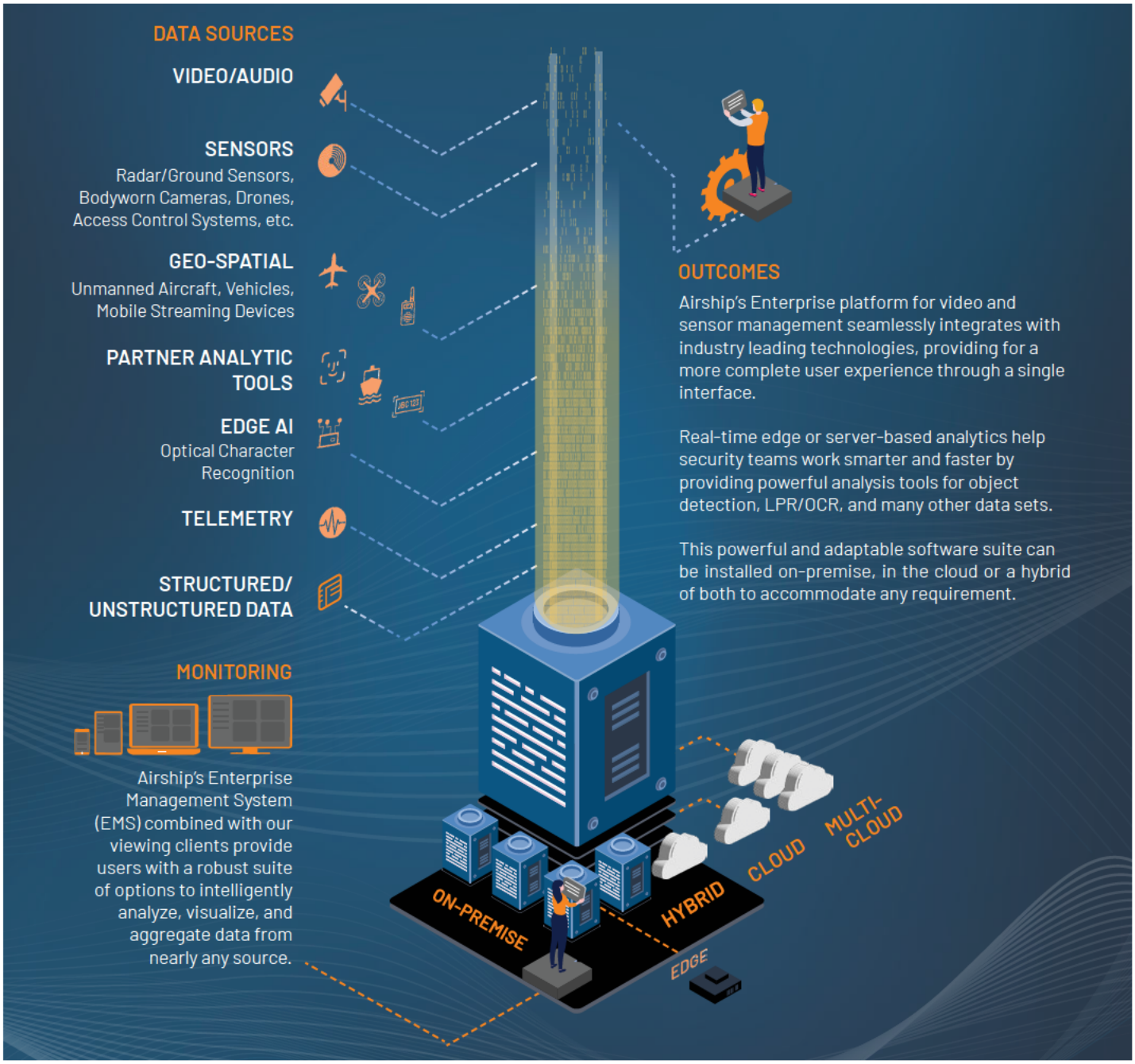
The deployment and use of any Airship product is subject to the terms and conditions defined in the Airship End User License Agreement (EULA). Please read the EULA for full details on the terms and conditions applicable to the specific Airship product.

AIRSHIP PRODUCT PRICING

Airship's simplified deployment model utilizes camera license pricing only, w th Airship EMS and or any software components that come within the EMS AIO software stack being provided at no additional cost. Airship can either bundle the cost of support with licensing or price separately.

For those users that do not require Airship EMS, such as a small deployment of less than 64 cameras, Airship Recording Server will be provided to manage all the cameras locally, at no cost, regardless of the number of Airship Recording Server licenses being provided.

Software Ecosystem Overview



©2022 Airship Industries

AIRSHIP ADVANTAGE

Airship Advantage is Airship's customer service and support program that provides (at minimum) complete coverage of all procured Airship products and services through our US-based support center in Redmond, WA. Airship Advantage comes in two (2) different packages, depending on the level of support needed and the scope of the products and services being procured.

Each Airship Advantage package comes with unlimited updates, patches, fixes, and new Airship software releases that are released within the period of performance covered. Airship Advantage begins the day products and/or services are delivered to the customer (except when a Period of Performance is defined).

All initial purchases of Airship products and services require an Airship Advantage package to be purchased at the time of the order, covering at minimum the first year of the product and or services deployment. Airship provides single and multiple year coverage options, up to five (5) years from the initial purchase.

If, or when additional products or services are purchased after the initial Airship Advantage plan is implemented, Airship can provide pro-rated pricing for the new products and services so that they keep the same expiration date as the initial purchase. Alternatively, Airship can initiate a new coverage plan at the same or different coverage level with its own expiration date.

In the event that the customer allows the Airship Advantage coverage to lapse at any point and would like to get said products and or services back under coverage at a later date, Airship will provide a quote that covers the period of time that the products and services were out of coverage, which must be executed prior to or at the same time that the new coverage plan is instituted.

Advantage Program	Support Availability	Support Coverage
Airship Gold Support	08:00AM to 8:00PM (EST)	Lens-to-Server
Airship Platinum Support	24/7/365	Lens-to-Server

Airship Gold Support

Airship Advantage Gold provides 08:00AM to 8:00PM (EST) "lens-to-server" customer service through our 1-800 technical support telephone number. Airship Advantage Gold provides support starting at the camera or edge sensor all the way back through the network to where the Airship software is installed. Where Airship can, we will identify, diagnose, and provide insight and or assistance with how to resolve the underlying problem.

Airship Platinum Support

Airship Advantage Platinum provides 24/7/365 "lens-to-server" customer service through our 1-800 technical support telephone number. Airship Advantage Platinum provides support starting at the camera or edge sensor all the way back through the network to where the Airship software is installed, identifying, and diagnosing the problem across the entire ecosystem. Where Airship can resolve the issue, it will, regardless of whether the issue is with Airship provided products or services.

AIRSHIP CAMERA LICENSE(S)

Airship's interchangeable camera licenses allow a single device/sensor to connect to the Airship ecosystem. A single camera license is required for each newly connected device/sensor that is configured to live stream. Camera licenses are valid in perpetuity and can be reassigned as devices and sensors are replaced, as Airship does not tie licenses to device MAC addresses. Licenses are not required for cameras that are added to the system and are not actively streaming or being recorded.

Airship camera and device licenses are offered in two (2) variations, Enterprise and Core. Airship Core licenses provide for a fully operational system for non-federated environments with standard camera and device integrations. Airship Enterprise licenses provide the same features and benefits as Professional licenses, with the additional benefits of enterprise federation, Case Management, LDAP Integration, Evidence Discover Server, advanced mapping features, and many more.

AIRSHIP ENTERPRISE MANAGEMENT SYSTEM (EMS)

Airship EMS connects unlimited cameras and devices within a single management interface, supporting single site locations, as well as global federated deployments. Airship EMS provides a simple and straight forward interface for managing cameras, devices / sensors, users, permissions, and system wide features such as fail-over and archiving, all from a wizard based graphical-user-interface (GUI).

Airship EMS is comprised of software components that can be installed physically or virtually as an all-in-one or broken out by component as desired by the customer to meet specific requirements. Airship's EMS software stack includes Airship Recording Server, Airship Nexus Video Portal, Airship Transcoding Server, Airship Relay Server, and other related components that may be required based on the customer's operating environment.

For more information about our Enterprise and Core software and licensing models please reach out to your Airship sales representative or email us at sales@airshipvms.com

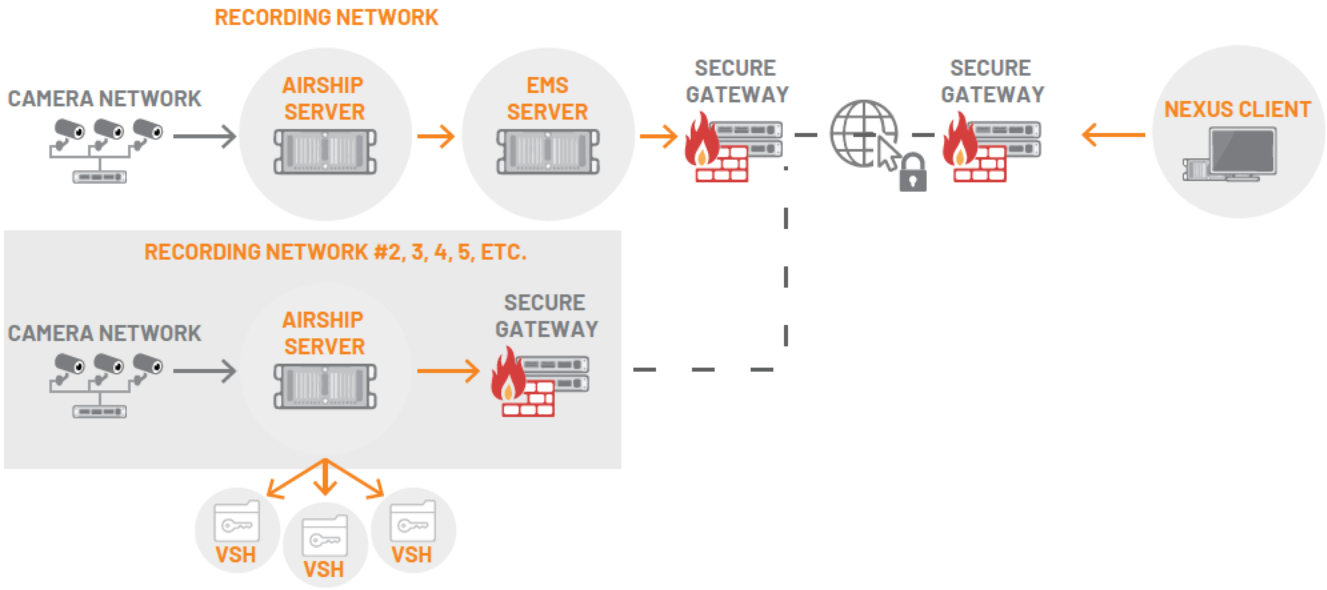
©2022 Airship Industries

Airship Server

The Recording Server is central to **Airship**, as it connects to cameras, sensors, and other devices to collect and record video, audio, and meta-data for permission-based distribution. This robust software is scalable for many use cases, delivering improved video/audio monitoring in both real-time and playback situations without compromising quality.

Airship Server can be installed as a standalone system (above) or be paired with other Airship Servers in a Managed or Unmanaged fashion. With Airship Server in unmanaged mode, users, cameras, and permissions are locally managed per Server. Each Server may be added to Nexus Client and viewed from any location accessible by network.

Additionally, Virtual Server Hosts (VSH) are segregated instances within Airship Server which may have unique permissions and cameras associated with each instance, allowing for maximum compartmentalization. Servers can be installed and managed regionally in large-scale deployments to cut down on latency and local management.



EDS

In addition to our Enterprise Management Server, Airship offers the Evidence Discovery Server (EDS) as a comprehensive tool for managing digital electronic evidence in a secure on-premise or cloud-based environment.



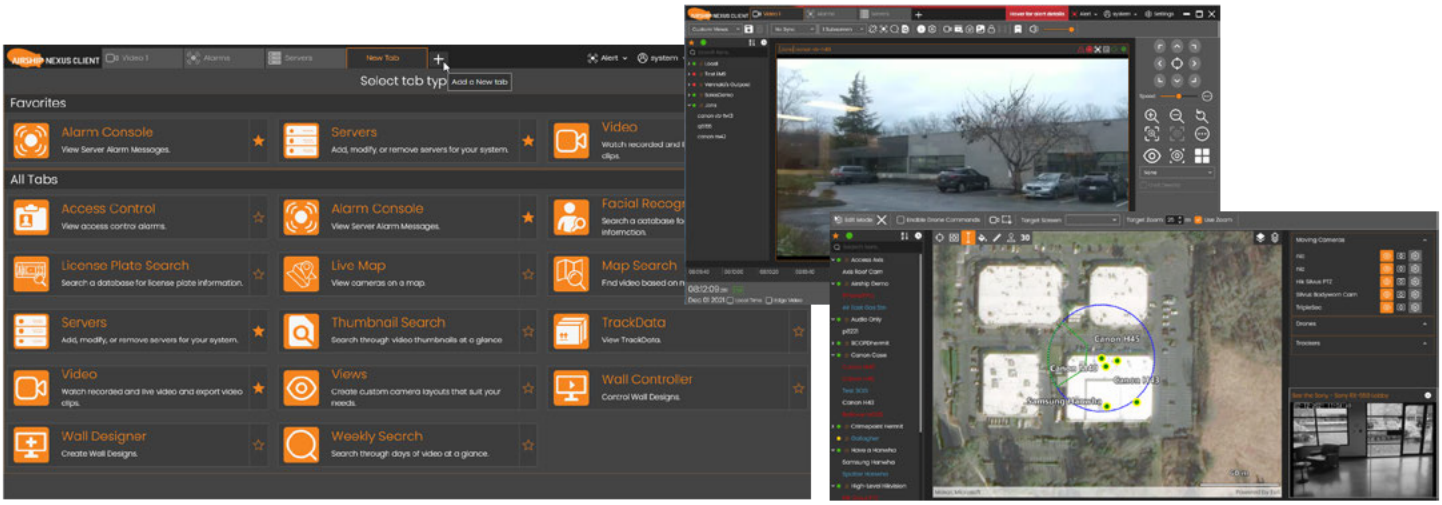
It allows for video review by legal personnel in a scalable, isolated, and secured environment separated from the active production recording solution, preventing any possibility of compromising the active evidence collection, while allowing a user-friendly environment for full review of post-recording audio/video.

AIRSHIP CLIENT PRODUCTS

Airship Nexus Client

This feature-rich viewing client enables user to view live and recorded footage, access alarm metadata, remotely configure cameras, pan/tilt/zoom, and numerous other features essential to surveillance monitoring. Installed on a desktop computer or laptop, this Windows software requires either a direct connection to the server's network or a valid VPN connection. The goal of Nexus Client is full control of camera feeds being recorded by Airship Server, while also offering remote server configuration capability.

Automatic notifications alert your team to incidents. Nexus Client then provides you with a robust set of tools for response, including: video export, screenshots and bookmarking. Nexus Client is a reliable remote configuration tool to manage camera settings and server settings, record templates, apply alarm analytics and more in real time.



Airship Nexus Video Portal

Airship Nexus Video Portal is the thin-client version of Nexus Client, providing a feature rich interface for accessing attached sensors and devices. Nexus Video Portal runs on any Internet-enabled device, including mobile devices, without requiring any software to be installed.



Airship Nexus Mobile

Like Nexus Client, the Nexus Mobile application allows you to maintain full control of camera feeds managed by Airship Server from your iOS or Android device. PTZ presets or camera views can be called upon for quick control. Picture-in-picture mode allows users to view live footage while reviewing playback footage simultaneously while still giving full playback controls.

Users can double-tap the screen while viewing a camera to take a screenshot, or save footage as Hosted clips, available for playback on Nexus Client, Nexus Video Portal, or locally on the app. Hosted clips may also be downloaded directly to the devices' camera roll.



©2022 Airship Industries

AIRSHIP EDGE PRODUCTS

Airship Outpost

Our Outpost AI device is a small form factor unit designed to increase high-quality data at the edge. Airship Outpost AI provides edge-based recording and encoding of video, audio, and sensor metadata from a wide range of devices. Airship Outpost AI utilizes a specialized video codec to encode and stream the edge-based sensor data back to a centrally managed server, providing a high level of efficiency and security. Outpost AI also records the native camera stream at the edge at a user defined recording profile, so that it can be retrieved physically later for evidentiary purposes or remotely pulled through the High-Resolution Download (HRDL) feature within Airship's Client software.



Airship Outpost Mobile

Airship Outpost Mobile is an installable application that runs on iOS and Android devices and can be found on Apple App Store or Google Marketplace. Outpost Mobile provides edge recording and encoding of video back to a central receive location, at a user-defined variable or fixed bit-rate, utilizing the tablet or handsets camera and microphone.

Outpost Mobile also records video locally at the edge to the tablet or handset, at a user-defined resolution and frame rate, which is then made available to the remote user via Airship's High Resolution Remote Download (HRDL) feature.

Airship Outpost Mobile is a separate licensed application, per edge deployment, and requires a corresponding Airship Camera License to receive the feed from the edge. Airship Outpost is purchased as a standalone software application and licensed for use on the system through EMS.



PRICING

AIRSHIP SOFTWARE PRICING

PART NUMBER	DESCRIPTION	PRICE
AIR-CAM-LIC-COR	Airship Core Device License. Includes Airship's Recording Server and underlying software applications required for a standard non-enterprise software deployment. Also includes standard camera and device drivers.	$200.00
AIR-CAM-LIC-ENT	Airship Enterprise Device License. Includes Airship's Enterprise Management System (EMS) application, and underlying software applications required for an enterprise software deployment. Also includes advanced device integrations, Case Management for technical operations, and Evidence Discovery Server.	$300.00
AIR-OUTPOST-MOBILE-LIC	Airship Outpost Mobile Encoder Device License. Allows connection of edge iOS or Android based device back to the Airship Enterprise Management System (EMS). Requires a managed camera license to stream, view and manage the stream.	$495.00
AIR-OUTPOST-SINGLE-LIC	Airship Outpost (software only) Single Device License. Allows connection of edge device running Outpost software back to Airship Enterprise Management System (EMS). Requires camera device license to receive and manage the stream being encoded at the edge.	$995.00
AIR-OUTPOST-MULTI-LIC	Airship Outpost (software only) Multi-Stream License. Up To eight (8) Streams. Allows connection of edge device running Outpost back to Airship Enterprise Management System (EMS). Requires matching number of camera device licenses to receive and manage the streams being encoded at the edge. All streams are individually encoded.	$2,495.00

IMPORTANT: All new software license purchases will require the purchase of Gold or Platinum Customer Care.

©2022 Airship Industries

OUTPOST APPLIANCE PRICING



PART NUMBER	DESCRIPTION	PRICE
AIR-OUTPOST-1CH-CORE	Single Device License (Single Stream). Includes Airship Outpost running on small form factor NVIDIA edge compute device built by Airship in the US (fully NDAA compliant). Configured to run stand alone at the edge or be connected back to Airship EMS for ingest, display, and recording of video and audio recorded at the edge. Requires matching number of camera device licenses in EMS to receive and manage the streams being encoded at the edge.	$2,995.00
AIR-OUTPOST-MULTI-CORE	Multi Device License (Up to Eight Streams). Includes Airship Outpost running on small form factor NVIDIA edge compute device built by Airship in the US (fully NDAA compliant). Configured to run stand alone at the edge or be connected back to Airship EMS for ingest, display, and recording of video and audio recorded at the edge. Requires matching number of camera device licenses in EMS to receive and manage the streams being encoded at the edge.	$3,995.00
AIR-OUTPOST-1CH-AI	Single Device License (Single Stream). Includes Airship Outpost running on small form factor NVIDIA edge compute device built by Airship in the US (fully NDAA compliant). Includes AI driven edge object detection and recognition for common OCR character sets. Configured to connect back to Airship EMS for ingest, display, and recording of video and audio recorded at the edge along with edge analytic meta-data. Requires matching number of camera device licenses in EMS to receive and manage the streams being encoded at the edge.	$4,995.00

ALPR STREAM PRICING

PART NUMBER	DESCRIPTION	PRICE
AIR-ALPR-1CH	Single Device License (Single Stream). Requires EMS Server for management of video and meta-data, an ALPR Engine, as well as Nexus Client to view the meta-data results which include the OCR character set along with Make, Model, and Color for vehicles.	$700.00

NOTE: ALPR services must be renewed annually.

IMPORTANT: All new ALPR software license purchases will require the purchase of Gold or Platinum Customer Care. ALPR software requires additional hardware for operation. Contact your Airship sales representative for additional information.

ALPR SERVER PRICING

PART NUMBER	DESCRIPTION	PRICE
AIR-ALPR-5-1G	Airship ALPR Server, five (5) Camera Licenses, Requires EMS Server. Includes five (5) ALPR licenses. ALPR licenses are valid for one year from date of delivery. One year of Gold Customer care included.	$7,445.00
AIR-ALPR-10-1G	Airship ALPR Server, ten (10) Camera Licenses, Requires EMS Server. Includes five (10) ALPR licenses. ALPR licenses are valid for one year from date of delivery. One year of Gold Customer care included.	$12,175.00
AIR-ALPR-25-1G	Airship ALPR Server, twenty-five (25) Camera Licenses, Requires EMS Server. Includes five (25) ALPR licenses. ALPR licenses are valid for one year from date of delivery. One year of Gold Customer care included.	$30,135.00

NOTE: ALPR services must be renewed annually.

©2022 Airship Industries

AIRSHIP SERVER PRICING

PART NUMBER	DESCRIPTION	PRICE
AIR-AIO-08-1U	1U EMS AIO, 8 Channel, OEM Server, Xeon 12 Core, SSD OS, Windows 2019, 32GB RAM, 32TB Storage. Camera licenses not provided. Please specify at time of order.	$8,400.00
AIR-AIO-16-1U	2U EMS AIO - 16 Channel, OEM Server, Xeon 16 Core, 32 GB Ram, Windows 2019, 54TB Storage. Camera licenses not provided. Please specify at time of order.	$11,746.00
AIR-AIO-16-2U	2U EMS AIO - 16 Channel, OEM Server, Xeon 16 Core, 32 GB Ram, Windows 2019, 40TB Storage. Camera licenses not provided. Please specify at time of order.	$12,838.00
AIR-AIO-32-2U	2U EMS AIO - 32 Channel, OEM Server, Xeon 16 Core, 32 GB Ram, Windows 2019, 80TB Storage. Camera licenses not provided. Please specify at time of order.	$13,930.00
AIR-AIO-64-2U	2U EMS AIO - 64 Channel, OEM Server, Xeon 16 Core, 32 GB Ram, Windows 2019, 160TB Storage. Camera licenses not provided. Please specify at time of order.	$16,366.00
AIR-WORK-A	Airship OEM Workstation, 6 Core CPU, 16GB RAM 1 Nvidia P400, Windows 10. Ideal for 2 x Monitor Configuration.	$1,995.00
AIR-WORK-B	Airship OEM Workstation, 10-Core CPU, 16, GB RAM, 2 Nvidia P400 GPU, Windows 10. Ideal for 4 x Monitor Configuration.	$3,416.00

IMPORTANT: All new Airship server purchases include Gold Customer Care. Custom hardware configurations available. Contact your Airship sales representative for additional information.

AIRSHIP ADVANTAGE - SUPPORT PRICING

IMPORTANT: Additional discounts off MSRP may apply depending on the support level, length of contract, and other factors determined by sale.

PART NUMBER	DESCRIPTION	PRICE
AIR-CAM-SUP-G	One year support and SMA for single stream camera license. GOLD SUPPORT.	$105.00
AIR-CAM-SUP-P	One year support and SMA for single stream camera license. PLATINUM SUPPORT.	$165.00
AIR-OUTPOST-MOBILE-SUP-G	One year support and SMA for single Outpost Mobile license. GOLD SUPPORT.	$173.00
AIR-OUTPOST-MOBILE-SUP-P	One year support and SMA for single Outpost Mobile license. PLATINUM SUPPORT.	$272.00
AIR-OUTPOST-SINGLE-SUP-G	One year support and SMA for single Outpost appliance license. GOLD SUPPORT.	$348.00
AIR-OUTPOST-SINGLE-SUP-P	One year support and SMA for single Outpost appliance license. PLATINUM SUPPORT.	$547.00
AIR-OUTPOST-MULTI-SUP-G	One year support and SMA for multi-stream Outpost appliance license. GOLD SUPPORT.	$873.00
AIR-OUTPOST-MULTI-SUP-P	One year support and SMA for multi-stream Outpost appliance license. PLATINUM SUPPORT.	$1,372.00

OUTPOST HARDWARE - SUPPORT

PART NUMBER	DESCRIPTION	PRICE
AIR-OUTPOST-1CH-CORE-SUP-G	One year support and SMA for single Outpost appliance license. GOLD SUPPORT.	$588.00
AIR-OUTPOST-1CH-CORE-SUP-P	One year support and SMA for single Outpost appliance license. PLATINUM SUPPORT.	$787.00
AIR-OUTPOST-MULTI-CORE-SUP-P	One year support and SMA for multi-stream Outpost appliance license. GOLD SUPPORT.	$765.00
AIR-OUTPOST-MULTI-CORE-SUP-P	One year support and SMA for multi-stream Outpost appliance license. PLATINUM SUPPORT.	$1,065.00
AIR-OUTPOST-1CH-AI-SUP-G	One year support and SMA for single stream Outpost AI appliance. GOLD SUPPORT.	$1,488.00
AIR-OUTPOST-1CH-AI-SUP-P	One year support and SMA for single stream Outpost AI appliance. PLATINUM SUPPORT.	$1,687.00

©2022 Airship Industries

AIRSHIP SERVER - SUPPORT

PART NUMBER	DESCRIPTION	PRICE
AIR-AIO-08-1U-SUP	One year of software support and SMA for Airship All-in-One 8-Channel 1U Server.	$1,260.00
AIR-AIO-16-1U-SUP	One year of software support and SMA for Airship All-in-One 16-Channel 1U Server.	$1,258.00
AIR-AIO-16-2U-SUP	One year of software support and SMA for Airship All-in-One 16-Channel 2U Server.	$1,375.00
AIR-AIO-32-2U-SUP	One year of software support and SMA for Airship All-in-One 32-Channel 2U Server.	$1,492.00
AIR-AIO-64-2U-SUP	One year of software support and SMA for Airship All-in-One 64-Channel 2U Server.	$1,753.00
AIR-WORK-A-SUP	One year of software support and SMA for Airship dual-monitor workstation.	$215.00
AIR-WORK-B-SUP	One year of software support and SMA for Airship quad-monitor workstation.	$366.00

IMPORTANT: Please consult with your Airship sales representative if multiple years of software and/or hardware support are required for your system.

©2022 Airship Industries

PROFESSIONAL SERVICES AND TRAINING

Airship provides a variety of tailored training and professional services. These services include:

- Applications consulting and engineering
- Configuration of redundant solutions
- Configuration of Enterprise Architecture systems
- Cleared personnel delivering System Administrative support
- Custom on-site training
- Services for non-Software Support Agreement customers and products not covered under warranty or SSA

PART NUMBER	DESCRIPTION	PRICE
AIR-ONSITE-SUP	On-site Professional Services; Per Diem	$2,500.00
AIR-ONSITE-UP-SUP	On-site Professional Services Uplift; Per Diem (AFTER HOURS/WEEKENDS)	$500.00
AIR-OFFSITE-SUP	Off-site/Remote Professional Services; Per Diem	$1,200.00
AIR-OFFSITE-UP-SUP	Off-site/Remote Professional Services Uplift; Per Diem (AFTER HOURS\ WEEKENDS)	$450.00
AIR-PHONE-SUP	Phone support for non-support customers; Two (2) hour minimum	$175.00
AIR-PHONE-UP-SUP	After hours phone support for non-support customers; Two (2) hour minimum	$300.00

[end]
rev:202204261417

Cruiser	Operator		User Training
[redacted]	[redacted]		11/17/2022
			11/17/2022
			11/17/2022
			11/17/2022
			12/10/2021

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this _____ day of _____, 2022 by and between the Department of State Police, hereinafter referred to as "Department," and the

_____,
a public entity, hereinafter referred to as "Agency," collectively referred to as "Parties."

WHEREAS, the Department contracts the services of one or more vendors to host an Automated License Plate Recognition (ALPR) database to store ALPR data; and

WHEREAS, the Parties provide public safety services within their respective jurisdictions; and

WHEREAS, the Parties have found it to be of mutual benefit to provide for the most efficient utilization of their resources and services in the application to public safety efforts within their respective jurisdictions; and

WHEREAS, the Parties are committed to cooperation and coordination in providing the highest level of public safety services to the public, guided by the principle that performing cooperatively is in the best interest of the public; and

WHEREAS, the Agency desires to use the ALPR system contracted and managed by the Department to facilitate the storage of ALPR information generated by the Agency; and

WHEREAS, the Agency desires to share law enforcement information owned by the Agency under the conditions set forth in this Agreement.

NOW, THEREFORE, for and in consideration of the covenants contained herein, IT IS HEREBY AGREED, by and between the Parties as follows:

1. PURPOSE:

The purpose of this Agreement is to provide a standardized approach and method of storage, retention, sharing, and access of ALPR data between the Department and Public Safety Agencies hosting ALPR data on the Department's ALPR system.

2. COSTS:

The Department shall be responsible for the costs of purchasing and maintaining the ALPR system as long as such funding is available to the Department and authorized by the appropriate authorities of the Commonwealth. Participating agencies shall be responsible for the costs of purchasing, servicing, maintaining, repairing, and/or licensing the ALPR equipment used by their respective agency. The Department shall not be responsible for any costs incurred by the Agency for the purchasing, servicing, maintaining, repairing, and/or licensing of the ALPR equipment owned or used by the Agency. The Agency shall inspect the Agency's ALPR equipment on a regular basis and document each inspection. Any irregularities or malfunctions of any ALPR equipment owned by the Agency or of any ALPR information shall be reported to the Department immediately and shall be addressed and repaired by the Agency as soon as reasonably possible.

3. DATA ACCESS AND SECURITY REQUIREMENTS:

a. System Availability: The Department will work with the vendor(s) to keep the ALPR system software and servers online and available with downtime limited to necessary system maintenance activities or to any outages that are beyond the control of the Department.

b. Data Sharing: ALPR data contributed by the Agency will be accessible for official purposes to all Agencies that have entered into an ALPR Agreement with the Department. The Agency shall not otherwise share ALPR data with or provide ALPR data to any person, entity, or government agency, other than a law enforcement agency, unless such disclosure is authorized by policy or court order or unless such disclosure is required by the Massachusetts Rules of Criminal Procedure or Rules of Superior Court governing discovery in criminal matters.

c. Security Requirements: The Department and the Agency agree to enforce and maintain security requirements for the information stored in the ALPR system as specified in the Agreement. The Agency agrees that the information hosted in the ALPR system shall be used for law enforcement purposes only and that only law enforcement agency employees that have been subject to appropriate background screening shall be allowed access to the system.

   Background screenings must be fingerprint-based and include check of both the state and national criminal history repositories. If a felony conviction of any kind is found, access to ALPR system shall not be granted. The Agency agrees not to share

passwords, user logins, or allow the ALPR software to be otherwise used by Agencies who have not entered into an Agreement with the Department allowing such activity.

An employee of the Agency may operate an ALPR unit that is connected to the Department's ALPR system or access the Department's ALPR system software only if the person has been designated as an authorized user by the Chief of the Agency or designee, and has received training from the Agency or the Department on the proper use and operation of ALPRs and any policy or procedures governing the use of ALPRs and ALPR data issued or adopted by the Agency.

4. IMPLEMENTATION OF POLICY:

The Agency shall, within 30 days of execution of this Agreement, adopt the Department's General Order TRF-11 as the policy and procedure document that will govern the Agency's use of and interaction with the Department's ALPR system. The Agency agrees that it has been provided with physical or electronic copy of General Order TRF-11, has had sufficient time to read, review, and understand the document in its entirety, and agrees to be bound by the provisions contained therein. The Department agrees to inform the Agency of any updates or modifications to General Order TRF-11, and the Agency understands and agrees that any updates to General Order TRF-11 will be binding upon the Agency unless the Agency elects to terminate the Agreement and withdraw from participation in the Department's ALPR system.

5. BENEFITS TO AGENCY:

a. Data Links: The centralized storage of ALPR data will provide a solution to the problem of inaccessible or irretrievable information due to disconnected ALPR systems and the difficulty in sharing information across jurisdictional boundaries.

b. Reduction of Costs: The centralized storage of ALPR data will reduce the financial burden to the Agency that is associated with purchasing and maintaining ALPR software.

6. RECORDS AND REPORTS:

The Department protects all ALPR information as personally identifiable information (PII) because ALPR information may be combined with other information to specifically identify a unique individual. As such, all information retained in the Department's ALPR system is the sole property of the Department. The Agency agrees that information stored in the ALPR system for the Agency may be subject to disclosure under certain circumstances. The Agency will refer to the Department for review all information requests for Agency information, including, but not

limited to, public records requests, court orders, legal motions, subpoenas, and/or summonses. The Department's Legal Department shall determine the best manner of responding to all requests for Agency information.

7. RETENTION

All ALPR information obtained by the Agency from the Department's ALPR system shall be retained pursuant to the Department's General Order TRF-11.

8. AMENDMENTS:

Any changes and additions to this Agreement shall be made by written amendments to this Agreement and shall not be effective until approved in writing by the Parties. A joint review of this Agreement may be requested at any time by either of the Parties to identify needed changes, which may be amended by written mutual agreement of the Parties.

9. DURABILITY:

This Agreement shall become operational and effective upon execution by the Parties. Parties may terminate the Agreement at any time by giving written notice to the other Parties at least thirty (30) days prior to the effective date of termination. The Agreement may also be terminated by the Department without prior notice to the Agency in the event of executive, legislative, or judicial mandate which requires the unanticipated discontinuation or modification of the ALPR program. In the event of such termination, the Department will notify the Agency as soon as practicable.

10. BENEFITS:

The Parties shall agree that the provisions of this Agreement are not intended to directly benefit and shall not be enforceable by any person or entity not a party to this Agreement. This Agreement is not intended to confer any legal rights or benefits on any person or entity other than the Parties of this Agreement.

11. INDEMNIFICATIONS:

Parties shall defend, indemnify, and hold harmless every other party and its officers, agents, employees, and representatives from any and all losses, liability, damages, claims, suits, actions and administrative proceedings, and demands and all expenditures and cost relating to acts or omissions of the indemnitor, its officers, agents, or employees arising out of or incidental to the

performance of any of the provisions of this Agreement. Parties do not assume liability for the acts or omissions of persons other than their respective officers, its employees, agents, and MOU officers.

The Agency releases the Department from any liability relating to the loss or destruction of data contributed by the Agency. The Agency further releases the Department from any liability relating to the loss of the Agency's access to the ALPR system due to system outage, commercial vendor failure or malfeasance, or executive, legislative, or judicial mandate which requires the unanticipated discontinuation or modification of the ALPR program. The Agency further releases the Department from any liability relating to the release of data or information contributed by the Agency pursuant to a lawful procedure or order.

12. ASSIGNMENT PROHIBITED:

Parties to this Agreement may not assign any right or obligation pursuant to this Agreement. Any attempted or purported assignment of any right or obligation pursuant to this Agreement shall be void and of no effect.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the date as written below.

_____	_____
Colonel Christopher S. Mason Massachusetts State Police	Representative: Agency:
_____	_____
Date	Date



ALL TRAFFIC
SOLUTIONS™

All Traffic Solutions

SPEED AND MESSAGE TRAILERS

AllTrafficSolutions.com

MADE IN THE USA

COMBAT YOUR TOUGHEST TRAFFIC, SAFETY AND MESSAGING CHALLENGES

With rugged, state-of-the-art trailers that are easy to maneuver as your needs change.

VERSATILITY

Our trailers are multipurpose tools that you can use to calm traffic, share information, collect traffic data, resolve speeding complaints, capture license plates, and more depending on which All Traffic Solutions (ATS) signs you choose to mount on them.

EASE OF USE

ATS trailers are thoughtfully engineered to be easy to use, transport, and deploy. The trailers feature a simple manual lever lift system for quick 1-person setup. No special equipment is needed to transport them— they can be towed by any size vehicle with a 2" receiver hitch.

RUGGED DURABILITY

Most ATS trailers are still in use after 10 or 15 years of year-round use. The continuous weld steel frame and marine-grade powder coat finish withstands heavy rain, snow, ice, and extreme temperatures without rusting.



ALPR-ready ATS 5 Trailer



SpeedAlert 18 on an ATS 3 Trailer



SpeedAlert 24 on an ATS 5 trailer



InstAlert 24 on an ATS 5 trailer

	Product Image	
ATS 3 TRAILER **Recommended Uses:** Traffic calming and sharing messages with drivers traveling at up to 45 miles per hour **Compatible Signs:** • Shield 12 and 15 radar speed signs • SpeedAlert 18 radar message sign • InstAlert 18 variable message sign		**Trailer-based Strobe Options:*** None **Dimensions:** 88.37" long × 56.43" wide × 84.4" tall **Sign Mounting:** Sign is mounted to a pole that can be rotated 360 degrees to point the sign in any desired direction
ATS 5 TRAILER **Recommended Uses:** Traffic calming and sharing messages with drivers traveling at up to 55 miles per hour **Compatible Signs:** • Shield 15 radar speed sign • SpeedAlert 18 and 24 radar message signs • InstAlert 18 and 24 variable message signs		**Trailer-based Strobe Options:*** Red and blue violator strobe bar **Dimensions:** 61.5" long x 62.5" wide x 90" tall **Sign Mounting:** Sign is stationary and forward-facing
ALPR-READY TRAILER **Recommended Uses:** Traffic calming, sharing messages with drivers traveling at up to 55 miles per hour, and capturing license plates **Compatible Signs:** • Shield 15 radar speed sign • SpeedAlert 18 and 24 radar message signs • InstAlert 18 and 24 variable message signs		**Trailer-based Strobe Options:*** Red and blue violator strobe bar **Dimensions:** 61.5" long x 62.5" wide x 90" tall **Sign Mounting:** Sign is stationary and forward-facing

**Note: the Shield Radar Speed Signs and SpeedAlert 18 Radar Speed Signs have strobes built in to the sign*

MADE IN THE USA

ABOUT ALL TRAFFIC SOLUTIONS

Since our inception in 2000, we have helped over 6,000 government agencies, higher education institutions, and private sector organizations manage traffic and improve overall safety.

MADE IN THE USA

Our signs and trailers are engineered and manufactured in the United States in compliance with the Buy America Act and the Buy American Act.

CUSTOMER EXPERIENCE

We are well-known in the industry for providing exceptional service to our customers. We proudly stand behind our products with US-based tech support, complimentary one-on-one product trainings, and the best warranty plans on the market, so you get the most out of your purchase for years to come.





For more information visit us online at AllTrafficSolutions.com

sales@alltrafficsolutions.com Call us at 866.366.6602

All Traffic Solutions. 14201 Sullyfield Circle, Suite 300, Chantilly, VA 20151

©All Traffic Solutions TraffiCloud® leverages our patented technology (US Patents 8417442; 8755990; 9070287; 9411893) to deliver unique cloud-based management, features and functionality. TraffiCloud® is a registered trademark of All Traffic Solutions.

All Traffic Solutions products are made in the USA in compliance with both the Buy America Act and the Buy American Act. All Traffic Solutions is a BuyBoard vendor for the BuyBoard National Purchasing Cooperative. We can provide Sole Source documentation for any products connected to TraffiCloud. A complete list of purchase options can be found on our website. GSA contract number: GS-07F-6092R

AutoVu SharpV

Automatic License Plate Recognition System

Crystal clear automatic license plate recognition in all conditions

Whether you want to scan vehicles on busy roadways, or to keep track of those accessing your facilities, you need a reliable system that performs in challenging conditions. The Genetec AutoVu™ SharpV provides crisp, full HD captures at all times. Day or night, in slow local streets, or on fast multi-lane highways, you can rest easy that it's gathering the insights you need when you need it most.

The SharpV goes beyond license plate identification. Its suite of vehicle analytics supports your investigations and helps you close cases faster. And thanks to its simplified design, it can be up and running in no time, letting you focus on your mission.



Key features

- Superior performance and new analytics with high-performance onboard machine learning
- See everything clearly with two ultra-wide sensors that provide quality images and capture data across multiple lanes*
- Excellent night-time performance with high power pulsed illuminators and global shutter
- Reduce installation and maintenance costs with motorized lenses with auto-focus for remote zoom & focus configuration
- Deploy anywhere with built-in 4G/LTE cellular radio option*
- Integrate with induction loops using its onboard I/O

Key benefits

Intelligence at the Edge – With hardware-accelerated processing on-board, the SharpV doesn't rely on remote servers for analysis. This eliminates latency and reduces the impact of ALPR on your network. And since it doesn't rely on external hardware, it provides uninterrupted performance – even when connectivity is unavailable.

Simplify design & deployment – Don't limit your ability to gather necessary data based on local infrastructure. With its embedded 4G/LTE communication option, motorized lenses with auto-focus, and support for both 24Vdc and PoE++ power, deploying the SharpV is easy and free of headaches.

Tap other systems – Combine ALPR data with video surveillance, access control, and more with Genetec Security Center. Break down the silos between your systems to increase operational intelligence and situational awareness, and do more with your ALPR system.

Gather data when it matters most – Not all crimes happen in broad daylight. With its built-in illuminators, global shutter, and high-resolution sensors, the SharpV leads the industry in performance at night and in challenging conditions.

* To verify 4G/LTE and dual-lane feature availability in your region, contact your Genetec representative.

Specifications

ALPR camera sensor
1920 × 1200 @ 30 fps; monochrome; global shutter

Capture range
9–148* ft (3–45* m)

Dimensions
Height: 63 mm (2.5 in), 68.6 mm (2.7 in) high with sunshield for black version; 101.6 mm (4.0 in) high with front antenna
Width: 192 mm (7.6 in)
Length: 214 mm (8.5 in)

Weight
5.53 lb (2.51 kg)

Illuminator
Pulsed LED illuminator for effective use in 0 lux (total darkness) environments
940nm, 850nm, 740nm, and 590nm illumination wavelengths available

Context camera sensor
1920 × 1200 @ 30 fps; color; global shutter

Available color(s)
Security White / Black

Operating temperature
-40°F to 149°F (-40°C to 65°C) ambient
Storage Temperature: -40°F to 185°F (-40°C to 85°C)

On-board analytics
Vehicle type, vehicle color, speed estimation, direction of travel, virtual loop, plate origin (state and country**), etc.

Power supply
PoE++ (Power over Ethernet) 802.3bt Type 3: 27 W typical, 40 W max
24 V input option: 24 V dc +/-15%, 25 W typical consumption, 37 W max

Satellite positioning***
GPS, Glonass, Beidou, Galileo, QZSS

Sealing (water/dust protection)
IEC 60529: IP66/IP67

Still image compression
JPEG compression for ALPR and Context still images

Data interface
LAN: 1 × 10/100/1000 Base-T Ethernet port
WWAN (select models and territories): 4G/LTE Category 4

Video streaming
H.264 @ up to 30 fps

Vibration & shock
IEC 60068-2-64: 5~100Hz | 0.5 g rms
IEC 60068-2-27: 10g | 16ms half-sine
MIL-STD-810H §514.8
Category 4 – Composite two-wheeled trailer

Impact
IEC 62262: IK09

Electromagnetic immunity & emissions
FCC | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR35 / EN55035

EMC directive (CE marking)
2014/30/EU

Safety
IEC/EN 62471. Photobiological safety of lamps and lamp systems. Exempt group.

External I/Os
2 inputs / 2 outputs (opto-isolated)

Mounting
Pole and wall mount included

* Contact Genetec for additional details
** Available only for some regions and services. Talk to your Genetec representative for details.
*** Requires 4G/LTE option.





Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2021. Genetec, AutoVu and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

UPDATED: 26 NOV 2021

Massachusetts Department of Transportation - Highway Division

Goods And Services Award **Amount Range: $500,000 and up**

Originating Office: Highway Operations **Contract #:** 111753

Contract Type: Award **Project ID:**

Project/Location: Statewide-Telecommunications

Vendor/Party Name: Bain Cor Inc

Vendor/Party Address: 763 South St
Holbrook, MA 02343

Original Max. Obligation: Rate **Completion Date/Duration:** 6/30/25

NTP Date: 07-01-2020 **Federal Aid Number:**

Description:
Vendor is to provide specialized Equipment, Parts & Services for Roadway Telecommunications, Intelligent Traffic systems (ITS), Integrated Project Control Systems (IPCS)

RFR: BD-20-1030-0P100-0P070-49476

cc Tony Wade

Submitted By:		**Approved By:**	
Sharon Rong		Joseph C. Foti Digitally signed by Joseph C. Foti Date: 2020.08.11 07:29:33 -04'00'	
	Date	Deputy Administrator/Chief of Operations	Date
christine hurley barnes Digitally signed by christine hurley barnes Date: 2020.08.10 14:40:43 -04'00'		Owen P. Kane	
Deputy Chief of Operations	Date	General Counsel	Date
n/R		n/R	
Budget/C.E.P.O.	Date	Highway Administrator	Date
Anna Dolata 8/26/20		n/r	
Director of Contracts & Records	Date	Secretary/CEO	Date

DOT AWARD 03-25-2010

Item Number: W-1

Date: 8/26/20

Charles D. Baker, Governor
Karyn E. Polito, Lieutenant Governor
Stephanie Pollack, Secretary & CEO
Jonathan L. Gulliver, Highway Administrator

massDOT
Massachusetts Department of Transportation
Highway Division

MASTER SERVICE AGREEMENT
NOTICE TO PROCEED

September 3, 2020

Bain Cor, Inc.
763 South Street
Holbrook, MA 02343

Contract Number: 111753
Action Item Date: August 26, 2020
Action Item Number: 1

Dear John Cordeiro,

Enclosed is a signed copy of your Master Service Agreement with the Massachusetts Department of Transportation, Highway Division.

This contract is relative to the Specialized Equipment, Parts & Services for Roadway Telecommunications, Intelligent Traffic systems (ITS), Integrated Project Control Systems (IPCS) statewide.

The duration of this contract shall be from July 1, 2020 until June 30, 2025.

Sincerely,

Anna Dolata

Anna Dolata
Supervisor, Contracts & Records

AD/mas

cc: Fiscal
Contracts & Records

E-Mail: Tony Wade
Christine Hurley-Barnes
Sharon Rong

Ten Park Plaza, Suite 5510, Boston, MA 02116
Tel: 857-368-9537, Fax: 857-368-0623
www.mass.gov/massdot

MASSDOT STANDARD CONTRACT FORM

This form is issued and published by the Massachusetts Department of Transportation (MassDOT or Department). Any changes to the official printed language of this form shall be void. Additional non-conflicting terms may be added by Attachment. Contractors may not require any additional agreements, engagement letters, contract forms or other additional terms as part of this Contract without prior Department approval. Click on hyperlinks for definitions, instructions and legal requirements that are incorporated by reference into this Contract.

CONTRACTOR LEGAL NAME: Bain Cor Inc (and d/b/a):	DEPARTMENT NAME: Massachusetts Department of Transportation MMARS Department Code: DOT
Legal Address: (W-9, W-4,T&C): 763 South St, Holbrook, MA 02343	Business Mailing Address: 10 Park Plaza Suite 7410, Boston, MA 02116
Contract Manager: John Cordeiro	Billing Address (if different):
E-Mail: jcordeiro@baincor.com	Contract Manager: Tony Wade
Phone: 339-987-5525 Fax: 339-987-5528	E-Mail: Tony.Wade@dot.state.ma.us
Contractor Vendor Code: VC0000506451	Phone: Fax:
Vendor Code Address ID (e.g. "AD001"): AD001. (Note: The Address Id Must be set up for EFT payments.)	MMARS Doc ID(s): 111753 RFR/Procurement or Other ID Number: BD-20-1030-0P100-0P070-49476

X NEW CONTRACT

PROCUREMENT OR EXCEPTION TYPE: (Check one option only)

__ Statewide Contract (OSD or an OSD-designated Department)
__ Collective Purchase (Attach OSD approval, scope, budget)
X Department Procurement (includes State or Federal grants 815 CMR 2.00) (Attach RFR and Response or other procurement supporting documentation)
__ Emergency Contract (Attach justification for emergency, scope, budget)
__ Contract Employee (Attach Employment Status Form, scope, budget)
__ Legislative/Legal or Other: (Attach authorizing language/justification, scope and budget)

___ CONTRACT AMENDMENT

Enter Current Contract End Date *Prior* to Amendment: _____, 20___.
Enter Amendment Amount: $ _____. (or "no change")

AMENDMENT TYPE: (Check one option only. Attach details of Amendment changes.)

__ Amendment to Scope or Budget (Attach updated scope and budget)
__ Interim Contract (Attach justification for Interim Contract and updated scope/budget)
__ Contract Employee (Attach any updates to scope or budget)
__ Legislative/Legal or Other: (Attach authorizing language/justification and updated scope and budget)

The following MassDOT TERMS AND CONDITIONS (T&C) has been executed, filed with CTR and is incorporated by reference into this Contract.

X MassDOT Terms and Conditions

COMPENSATION: (Check ONE option): The Department certifies that payments for authorized performance accepted in accordance with the terms of this Contract will be supported in the state accounting system by sufficient appropriations or other non-appropriated funds, subject to intercept for MassDOT/Commonwealth owed debts under 815 CMR 9.00.
X Rate Contract (No Maximum Obligation. Attach details of all rates, units, calculations, conditions or terms and any changes if rates or terms are being amended.)
__ Maximum Obligation Contract Enter Total Maximum Obligation for total duration of this Contract (or ***new*** Total if Contract is being amended). $ _____

PROMPT PAYMENT DISCOUNTS (PPD): Commonwealth payments are issued through EFT 45 days from invoice receipt. Contractors requesting **accelerated** payments must identify a PPD as follows: Payment issued within 10 days 2 % PPD; Payment issued within 15 days _____ % PPD; Payment issued within 20 days _____ % PPD; Payment issued within 30 days _____% PPD. If PPD percentages are left blank, identify reason: __ agree to standard 45 day cycle __ statutory/legal or Ready Payments (G.L. c. 29, § 23A); __ only initial payment (subsequent payments scheduled to support standard EFT 45 day payment cycle. See Prompt Pay Discounts Policy.)

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE or REASON FOR AMENDMENT: (Enter the Contract title, purpose, fiscal year(s) and a detailed description of the scope of performance or what is being amended for a Contract Amendment. Attach all supporting documentation and justifications.)
Vendors are to provide specialized Equipment, Parts & Services for Roadway Telecommunications, Intelligent Traffic systems (ITS), Integrated Project Control Systems (IPCS)

ANTICIPATED START DATE: (Complete ONE option only) The Department and Contractor certify for this Contract, or Contract Amendment, that Contract obligations:

__ 1. may be incurred as of the Effective Date (latest signature date below) and **no** obligations have been incurred **prior** to the Effective Date.
__ 2. may be incurred as of _____, 20__, a date **LATER** than the Effective Date below and **no** obligations have been incurred **prior** to the Effective Date.
X 3. were incurred as of **July 1, 2020**, a date **PRIOR** to the Effective Date below, and the parties agree that payments for any obligations incurred prior to the Effective Date are authorized to be made either as settlement payments or as authorized reimbursement payments, and that the details and circumstances of all obligations under this Contract are attached and incorporated into this Contract. Acceptance of payments forever releases the Commonwealth and MassDOT from further claims related to these obligations.

CONTRACT END DATE: Contract performance shall terminate as of **June 30, 2025**, with no new obligations being incurred after this date unless the Contract is properly amended, provided that the terms of this Contract and performance expectations and obligations shall survive its termination for the purpose of resolving any claim or dispute, for completing any negotiated terms and warranties, to allow any close out or transition performance, reporting, invoicing or final payments, or during any lapse between amendments.

CERTIFICATIONS: Notwithstanding verbal or other representations by the parties, the **"Effective Date"** of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified above, subject to any required approvals. The Contractor makes all certifications required under the attached Contractor Certifications (incorporated by reference if not attached hereto) under the pains and penalties of perjury, agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein according to the following hierarchy of document precedence, the MassDOT Terms and Conditions http://transnet/docs/ComApp/MassDOTTermsandConditions.doc, this Standard Contract Form including the Instructions and Contractor Certifications, the Request for Response (RFR) or other solicitation, the Contractor's Response, and additional negotiated terms, provided that additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.

AUTHORIZING SIGNATURE FOR THE CONTRACTOR:

X: John Cordeiro Date: 8/6/2020
(Signature and Date Must Be Handwritten At Time of Signature)
Print Name: JOHN CORDEIRO
Print Title: Vice President

AUTHORIZING SIGNATURE FOR MassDOT:

X: Joseph C. Foti Digitally signed by Joseph C. Foti Date: 2020.08.11 07:29:57 -04'00' Date:
(Signature and Date Must Be Handwritten At Time of Signature)
Print Name: Joseph Foti
Print Title: Deputy Administrator/Chief of Operations

INSTRUCTIONS AND CONTRACTOR CERTIFICATIONS

The following instructions and terms are incorporated by reference and apply to this Standard Contract Form. Text that appears underlined indicates a "hyperlink" to an internet or bookmarked site and are unofficial versions of these documents and Departments and Contractors should consult with their legal counsel to ensure compliance with all legal requirements. Using the Web Toolbar will make navigation between the form and the hyperlinks easier. Please note that not all applicable laws have been cited.

CONTRACTOR LEGAL NAME (AND D/B/A): Enter the **Full Legal Name** of the Contractor's business as it appears on the Contractor's W-9 or W-4 Form (Contract Employees only) **and** the MassDOT Terms and Conditions If Contractor also has a "doing business as" (d/b/a) name, BOTH the legal name and the "d/b/a" name must appear in this section.

Contractor Legal Address: Enter the Legal Address of the Contractor as it appears on the Contractor's W-9 or W-4 Form (Contract Employees only) **and** the MassDOT Terms and Conditions, which must match the legal address on the 1099I table in MMARS (or the Legal Address in HR/CMS for Contract Employee).

Contractor Contract Manager: Enter the authorized Contract Manager who will be responsible for managing the Contract. The Contract Manager should be an Authorized Signatory or, at a minimum, a person designated by the Contractor to represent the Contractor, receive legal notices and negotiate ongoing Contract issues. The Contract Manager is considered "Key Personnel" and may not be changed without the prior written approval of the Department. If the Contract is posted on COMMBUYS, the name of the Contract Manager must be included in the Contract on COMMBUYS.

Contractor E-Mail Address/Phone/Fax: Enter the electronic mail (e-mail) address, phone and fax number of the Contractor Contract Manager. This information must be kept current by the Contractor to ensure that the Department can contact the Contractor and provide any required legal notices. Notice received by the Contract Manager (with confirmation of actual receipt) through the listed address, fax number(s) or electronic mail address will meet any written legal notice requirements.

Contractor Vendor Code: The Department must enter the MMARS **Vendor Code** assigned by the Commonwealth. If a Vendor Code has not yet been assigned, leave this space blank and the Department will complete this section when a Vendor Code has been assigned. The Department is responsible under the Vendor File and W-9s Policy for verifying with authorized signatories of the Contractor, as part of contract execution, that the legal name, address and Federal Tax Identification Number (TIN) in the Contract documents match the state accounting system.

Vendor Code Address ID: (e.g., "AD001") The Department must enter the MMARS Vendor Code Address Id identifying the payment remittance address for Contract payments, which MUST be set up for EFT payments PRIOR to the first payment under the Contract in accordance with the Bill Paying and Vendor File and W-9 policies.

COMMONWEALTH DEPARTMENT NAME: Enter the full Department name with the authority to obligate funds encumbered for the Contract.

Commonwealth MMARS Alpha Department Code: Enter the three (3) letter MMARS Code assigned to this Commonwealth Department in the state accounting system.

Department Business Mailing Address: Enter the address where all formal correspondence to the Department must be sent. Unless otherwise specified in the Contract, legal notice sent or received by the Department's Contract Manager (with confirmation of actual receipt) through the listed address, fax number(s) or electronic mail address for the Contract Manager will meet any requirements for legal notice.

Department Billing Address: Enter the Billing Address or email address if invoices must be sent to a different location. Billing or confirmation of delivery of performance issues should be resolved through the listed Contract Managers.

Department Contract Manager: Identify the authorized Contract Manager who will be responsible for managing the Contract, who should be an authorized signatory or an employee designated by the Department to represent the Department to receive legal notices and negotiate ongoing Contract issues.

Department E-Mail Address/Phone/Fax: Enter the electronic mail (e-mail) address, phone and fax number of the Department Contract Manager. Unless otherwise specified in the Contract, legal notice sent or received by the Contract Manager (with confirmation of actual receipt) through the listed address, fax number(s) or electronic mail address will meet any requirements for written notice under the Contract.

MMARS Document ID(s): Enter the MMARS 20 character encumbrance transaction number associated with this Contract which must remain the same for the life of the Contract. If multiple numbers exist for this Contract, identify all Doc Ids.

RFR/Procurement or Other ID Number or Name: Enter the Request for Response (RFR) or other Procurement Reference number, Contract ID Number or other reference/tracking number for this Contract or Amendment and will be entered into the Board Award Field in the MMARS encumbrance transaction for this Contract.

NEW CONTRACTS (left side of Form):

Complete this section ONLY if this Contract is brand new. (Complete the CONTRACT AMENDMENT section for any material changes to an existing or an expired Contract, and for exercising options to renew or annual contracts under a multi-year procurement or grant program.)

PROCUREMENT OR EXCEPTION TYPE: Check the appropriate type of procurement or exception for this Contract. Only one option can be selected. See State Finance Law and General Requirements, Acquisition Policy and Fixed Assets, the Commodities and Services Policy and the Procurement Information Center (Department Contract Guidance) for details.

Statewide Contract (OSD or an OSD-designated Department). Check this option for a Statewide Contract under OSD, or by an OSD-designated Department.

Collective Purchase approved by OSD. Check this option for Contracts approved by OSD for collective purchases through federal, state, local government or other entities.

Department Contract Procurement. Check this option for a Department procurement including state grants and federal sub-grants under 815 CMR 2.00 and State Grants and Federal Subgrants Policy, Departmental Master Agreements (MA). If multi-Department user Contract, identify multi-Department use is allowable in Brief Description.

Emergency Contract. Check this option when the Department has determined that an unforeseen crisis or incident has arisen which requires or mandates immediate purchases to avoid substantial harm to the functioning of government or the provision of necessary or mandated services or whenever the health, welfare or safety of clients or other persons or serious damage to property is threatened.

Contract Employee. Check this option when the Department requires the performance of an Individual Contractor, and when the planned Contract performance with an Individual has been classified using the Employment Status Form (prior to the Contractor's selection) as work of a Contract Employee and not that of an Independent Contractor.

Legislative/Legal or Other. Check this option when legislation, an existing legal obligation, prohibition or other circumstance exempts or prohibits a Contract from being competitively procured, or identify any other procurement exception not already listed. Legislative "earmarks" exempt the Contract solely from procurement requirements, and all other Contract and state finance laws and policies apply. Supporting documentation must be attached to explain and justify the exemption.

CONTRACT AMENDMENT (Right Side of Form)

Complete this section for any Contract being renewed, amended or to continue a lapsed Contract. All Contracts with available options to renew must be amended referencing the original procurement and Contract doc ids, since all continuing contracts must be maintained in the same Contract file (even if the underlying appropriation changes each fiscal year.) "See Amendments, Suspensions, and Termination Policy.)

Enter Current Contract End Date: Enter the termination date of the Current Contract being amended, even if this date has already passed. (Note: Current Start Date is not requested since this date does not change and is already recorded in MMARS.)

Enter Amendment Amount: Enter the amount of the Amendment increase or decrease to a Maximum Obligation Contract. Enter "no change" for Rate Contracts or if no change.

AMENDMENT TYPE: Identify the type of Amendment being done. Documentation supporting the updates to performance and budget must be attached. **Amendment to Scope or Budget.** Check this option when renewing a Contract or executing any Amendment ("material change" in Contract terms) even if the Contract has lapsed. The parties may negotiate a change in any element of Contract performance or cost identified in the RFR or the Contractor's response which results in lower costs, or a more cost-effective or better value performance than was presented in the original selected response, provided the negotiation results in a better value within the scope of the RFR than what was proposed by the Contractor in the original selected response. Any "material" change in the Contract terms must be memorialized in a formal Amendment even if a corresponding MMARS transaction is not needed to support the change. Additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.

Interim Contracts. Check this option for an Interim Contract to prevent a lapse of Contract performance whenever an existing Contract is being re-procured but the new procurement has not been completed, to bridge the gap during implementation between an expiring and a new procurement, or to contract with an interim Contractor when a current Contractor is unable to complete full performance under a Contract.

Contract Employee. Check this option when the Department requires a renewal or other amendment to the performance of a Contract Employee.

Legislative/Legal or Other. Check this option when legislation, an existing legal obligation, prohibition or other circumstance exempts or prohibits a Contract from being competitively procured, or identify any other procurement exception not already listed. Legislative "earmarks" exempt the Contract solely from procurement requirements, and all other Contract and state finance laws and policies apply. Attach supporting documentation to explain and justify the exemption and whether Contractor selection has been publicly

posted.

MASSDOT TERMS AND CONDITIONS

The MassDOT Terms and Conditions has been executed by the Contractor and is incorporated by reference into this Contract. This Form is signed only once and recorded on the Vendor Customer File (VCUST). See Vendor File and W-9s Policy.

COMPENSATION

Identify if the Contract is a **Rate Contract** (with no stated Maximum Obligation) or a **Maximum Obligation Contract** (with a stated Maximum Obligation) and identify the Maximum Obligation. If the Contract is being amended, enter the new Maximum Obligation based upon the increase or decreasing Amendment. The Total Maximum Obligation must reflect the total funding for the dates of service under the contract, including the Amendment amount if the Contract is being amended. The Maximum Obligation must match the MMARS encumbrance. Funding and allotments must be verified as available and encumbered prior to incurring obligations. If a Contract includes both a Maximum Obligation component and Rate Contract component, check off both, specific Maximum Obligation amounts or amended amounts and Attachments must clearly outline the Contract breakdown to match the encumbrance.

PAYMENTS AND PROMPT PAY DISCOUNTS

Payments are processed within a 45 day payment cycle through EFT in accordance with the Commonwealth Bill Paying Policy for investment and cash flow purposes. Departments may NOT negotiate accelerated payments and Payees are NOT entitled to accelerated payments UNLESS a prompt payment discount (PPD) is provided to support the Commonwealth's and MassDOT's loss of investment earnings for this earlier payment, or unless a payments is legally mandated to be made in less than 45 days (e.g., construction contracts, Ready Payments under G.L. c. 29, s. 23A). See Prompt Pay Discounts Policy. PPD are identified as a percentage discount which will be automatically deducted when an accelerated payment is made. Reduced contracts rates may not be negotiated to replace a PPD. If PPD fields are left blank please identify that the Contractor agrees to the standard 45 day cycle; a statutory/legal exemption such as Ready Payments (G.L. c. 29, § 23A); or only an initial accelerated payment for reimbursements or start up costs for a grant, with subsequent payments scheduled to support standard EFT 45 day payment cycle. Financial hardship is not a sufficient justification to accelerate cash flow for *all* payments under a Contract. Initial grant or contract payments may be accelerated for the *first* invoice or initial grant installment, but subsequent periodic installments or invoice payments should be scheduled to support the Payee cash flow needs and the standard 45 day EFT payment cycle in accordance with the Bill Paying Policy. Any accelerated payment that does not provide for a PPD must have a legal justification in Contract file for audit purposes explaining why accelerated payments were allowable without a PPD.

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE

Enter a brief description of the Contract performance, project name and/or other identifying information for the Contract to specifically identify the Contract performance, match the Contract with attachments, determine the appropriate expenditure code (as listed in the Expenditure Classification Handbook) or to identify or clarify important information related to the Contract such as the Fiscal Year(s) of performance (ex. "FY2012" or "FY2012-14"). Identify settlements or other exceptions and attach more detailed justification and supporting documents. Enter "Multi-Department Use" if other Departments can access procurement. For Amendments, identify the purpose and what items are being amended. Merely stating "see attached" or referencing attachments without a narrative description of performance is insufficient.

ANTICIPATED START DATE

The Department and Contractor must certify WHEN obligations under this Contract/Amendment may be incurred. Option 1 is the default option when performance may begin as of the Effective Date (latest signature date and any required approvals). If the parties want a new Contract or renewal to begin as of the upcoming fiscal year then list the fiscal year(s) (ex. "FY2012" or "FY2012-14") in the Brief Description section. Performance starts and encumbrances reflect the default Effective Date (if no FY is listed) or the later FY start date (if a FY is listed). Use Option 2 only when the Contract will be signed well in advance of the start date and identify a specific future start date. Do not use Option 2 for a fiscal year start unless it is certain that the Contract will be signed prior to fiscal year. Option 3 is used in lieu of the Settlement and Release Form when the Contract/Amendment is signed late, and obligations have already been incurred by the Contractor prior to the Effective Date for which the Department has either requested, accepted or deemed legally eligible for reimbursement, and the Contract includes supporting documents justifying the performance or proof of eligibility, and approximate costs. Any obligations incurred outside the scope of the Effective Date under any Option listed, even if the incorrect Option is selected, shall be automatically deemed a settlement included under the terms of the Contract and upon payment to the Contractor will release the Commonwealth and MassDOT from further obligations for the identified performance. All settlement payments require justification and must be under same encumbrance and object codes as the Contract payments. Performance dates are subject to G.L. c.4, § 9.

CONTRACT END DATE

The Department must enter the date that Contract performance will terminate. **If the Contract is being amended and the Contract End Date is not changing, this date must be re-entered again here.** A Contract must be signed for at least the initial duration but not longer than the period of procurement listed in the RFR, or other solicitation document (if applicable). No new performance is allowable beyond the end date without an amendment, but the Department may allow a Contractor to complete minimal close out performance obligations if substantial performance has been made prior to the termination date of the Contract and prior to the end of the fiscal year in which payments are appropriated, provided that any close out performance is subject to appropriation and funding limits under state finance law, and CTR may adjust encumbrances and payments in the state accounting system to enable final close out payments. Performance dates are subject to G.L. c.4, § 9.

CERTIFICATIONS AND EXECUTION

See Department Head Signature Authorization Policy and the Contractor Authorized Signatory Listing for policies on Contractor and Department signatures.

Authorizing Signature for Contractor/Date: The Authorized Contractor Signatory must (in their own handwriting and in ink) sign AND enter the date the Contract is signed. See section above under "Anticipated Contract Start Date". Acceptance of payment by the Contractor shall waive any right of the Contractor to claim the Contract/Amendment is not valid and the Contractor may not void the Contract. **Rubber stamps, typed or other images are not acceptable.** Proof of Contractor signature authorization on a **Contractor Authorized Signatory Listing** may be required by the Department if not already on file.

Contractor Name /Title: The Contractor Authorized Signatory's name and title must appear legibly as it appears on the **Contractor Authorized Signatory Listing**.

Authorizing Signature For Department/Date: The Authorized Department Signatory must (in their own handwriting and in ink) sign AND enter the date the Contract is signed. See section above under "Anticipated Start Date". **Rubber stamps, typed or other images are not accepted.** The Authorized Signatory must be an employee within the Department legally responsible for the Contract. See Department Head Signature Authorization. The Department must have the legislative funding appropriated for all the costs of this Contract or funding allocated under an approved Interdepartmental Service Agreement (ISA). A Department may not contract for performance to be delivered to or by another state department without specific legislative authorization (unless this Contract is a Statewide Contract). For Contracts requiring Secretariat signoff, evidence of Secretariat signoff must be included in the Contract file.

Department Name /Title: Enter the Authorized Signatory's name and title legibly.

CONTRACTOR CERTIFICATIONS AND LEGAL REFERENCES

Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified, subject to any required approvals. The Contractor makes all certifications required under this Contract under the pains and penalties of perjury, and agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein:

MassDOT and Contractor Ownership Rights. The Contractor certifies and agrees that MassDOT is entitled to ownership and possession of all "deliverables" purchased or developed with Contract funds. A Department may not relinquish rights to deliverables nor may Contractors sell products developed with MassDOT resources without just compensation. The Contract should detail all MassDOT deliverables and ownership rights and any Contractor proprietary rights.

Qualifications. The Contractor certifies it is qualified and shall at all times remain qualified to perform this Contract; that performance shall be timely and meet or exceed industry standards for the performance required, including obtaining requisite licenses, registrations, permits, resources for performance, and sufficient professional, liability; and other appropriate insurance to cover the performance. If the Contractor is a business, the Contractor certifies that it is listed under the Secretary of State's website as licensed to do business in Massachusetts, as required by law.

Business Ethics and Fraud, Waste and Abuse Prevention. The Contractor certifies that performance under this Contract, in addition to meeting the terms of the Contract, will be made using ethical business standards and good stewardship of taxpayer and other public funding and resources to prevent fraud, waste and abuse.

Collusion. The Contractor certifies that this Contract has been offered in good faith and without collusion, fraud or unfair trade practices with any other person, that any actions to avoid or frustrate fair and open competition are prohibited by law, and shall be grounds for rejection or disqualification of a Response or termination of this Contract.

Public Records and Access The Contractor shall provide full access to records related to performance and compliance to the Department and officials listed under Executive Order 195 and G.L. c. 11, s.12 seven (7) years beginning on the first day after the final payment

under this Contract or such longer period necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving this Contract. Access to view Contractor records related to any breach or allegation of fraud, waste and/or abuse may not be denied and Contractor can not claim confidentiality or trade secret protections solely for viewing but not retaining documents. Routine Contract performance compliance reports or documents related to any alleged breach or allegation of non-compliance, fraud, waste, abuse or collusion may be provided electronically and shall be provided at Contractor's own expense. Reasonable costs for copies of non-routine Contract related records shall not exceed the rates for public records under 950 C.M.R. 32.00.

Debarment. The Contractor certifies that neither it nor any of its subcontractors are currently debarred or suspended by the federal or state government under any law or regulation including, Executive Order 147; G.L. c. 29, s. 29F G.L. c.30, § 39R, G.L. c.149, § 27C, G.L. c.149, § 44C, G.L. c.149, § 148B and G.L. c. 152, s. 25C.

Applicable Laws. The Contractor shall comply with all applicable state laws and regulations including but not limited to the applicable Massachusetts General Laws; the Official Code of Massachusetts Regulations; Code of Massachusetts Regulations (unofficial); 801 CMR 21.00 (Procurement of Commodity and Service Procurements, Including Human and Social Services); 815 CMR 2.00 (Grants and Subsidies); 808 CMR 1.00 (Compliance, Reporting and Auditing for Human And Social Services); AICPA Standards; confidentiality of Department records under G.L. c. 66A; and the Massachusetts Constitution Article XVIII if applicable.

Invoices. The Contractor must submit invoices in accordance with the terms of the Contract and the Commonwealth Bill Paying Policy. Contractors must be able to reconcile and properly attribute concurrent payments from multiple Departments. Final invoices in any fiscal year must be submitted no later than August 15th for performance made and received (goods delivered, services completed) prior to June 30th, in order to make payment for that performance prior to the close of the fiscal year to prevent reversion of appropriated funds. Failure to submit timely invoices by August 15th or other date listed in the Contract shall authorize the Department to issue an estimated payment based upon the Department's determination of performance delivered and accepted. The Contractor's acceptance of this estimated payment releases the Commonwealth and MassDOT from further claims for these invoices. If budgetary funds revert due to the Contractor's failure to submit timely final invoices, or for disputing an estimated payment, the Department may deduct a penalty up to 10% from any final payment in the next fiscal year for failure to submit timely invoices.

Payments Subject To Appropriation. Pursuant to G.L. c. 29 § 26, § 27 and § 29, Departments are required to expend funds only for the purposes set forth by the Legislature and within the funding limits established through appropriation, allotment and subsidiary, including mandated allotment reductions triggered by G.L. c. 29, § 9C. A Department cannot authorize or accept performance in excess of an existing appropriation and allotment, or sufficient non-appropriated available funds. Any oral or written representations, commitments, or assurances made by the Department or any other Commonwealth representative are not binding. The Commonwealth and MassDOT have no legal obligation to compensate a Contractor for performance that is not requested and is intentionally delivered by a Contractor outside the scope of a Contract. Contractors should verify funding prior to beginning performance.

Intercept. Contractors may be registered as Customers in the Vendor file if the Contractor owes a Commonwealth debt. Unresolved and undisputed debts, and overpayments of Contract payments that are not reimbursed timely shall be subject to intercept pursuant to G.L. c. 7A, s. 3 and 815 CMR 9.00. Contract overpayments will be subject to immediate intercept or payment offset. The Contractor may not penalize any state Department or assess late fees, cancel a Contract or other services if amounts are intercepted or offset due to recoupment of an overpayment, outstanding taxes, child support, other overdue debts or Contract overpayments.

Tax Law Compliance. The Contractor certifies under the pains and penalties of perjury tax compliance with Federal tax laws; state tax laws including but not limited to G.L. c. 62C, G.L. c. 62C, s. 49A; compliance with all state tax laws, reporting of employees and contractors, withholding and remitting of tax withholdings and child support and is in good standing with respect to all state taxes and returns due; reporting of employees and contractors under G.L. c. 62E, withholding and remitting child support including G.L. c. 119A, s. 12; TIR 05-11; New Independent Contractor Provisions and applicable TIRs.

Bankruptcy, Judgments, Potential Structural Changes, Pending Legal Matters and Conflicts. The Contractor certifies it has not been in bankruptcy and/or receivership within the last three calendar years, and the Contractor certifies that it will immediately notify the Department in writing **at least 45 days prior** to filing for bankruptcy and/or receivership, any potential structural change in its organization, or if there is **any risk** to the solvency of the Contractor that may impact the Contractor's ability to timely fulfill the terms of this Contract or Amendment. The Contractor certifies that at any time during the period of the Contract the Contractor is required to affirmatively disclose in writing to the Department Contract Manager the details of any judgment, criminal conviction, investigation or litigation pending against the Contractor or any of its officers, directors, employees, agents, or subcontractors, including any potential conflicts of interest of which the Contractor has knowledge, or learns of during the Contract term. Law firms or Attorneys providing legal services are required to identify any potential conflict with representation of any Department client in accordance with Massachusetts Board of Bar Overseers (BBO) rules.

Federal Anti-Lobbying and Other Federal Requirements. If receiving federal funds, the Contractor certifies compliance with federal anti-lobbying requirements including 31 USC 1352; other federal requirements; Executive Order 11246; Air Pollution Act; Federal Water Pollution Control Act and Federal Employment Laws.

Protection of Personal Data and Information. The Contractor certifies that all steps will be taken to ensure the security and confidentiality of all Commonwealth/MassDOT data for which the Contractor becomes a holder, either as part of performance or inadvertently during performance, with special attention to restricting access, use and disbursement of personal data and information under G.L. c. 93H and c. 66A and Executive Order 504. The Contractor is required to comply with G.L. c. 93I for the proper disposal of all paper and electronic media, backups or systems containing personal data and information, provided further that the Contractor is required to ensure that any personal data or information transmitted electronically or through a portable device be properly encrypted using (at a minimum) Information Technology Division (ITD) Protection of Sensitive Information, provided further that any Contractor having access to credit card or banking information of Commonwealth/MassDOT customers certifies that the Contractor is PCI compliant in accordance with the Payment Card Industry Council Standards and shall provide confirmation compliance during the Contract, provide further that the Contractor shall immediately notify the Department in the event of any security breach including the unauthorized access, disbursement, use or disposal of personal data or information, and in the event of a security breach, the Contractor shall cooperate fully with the Commonwealth/MassDOT and provide access to any information necessary for the Commonwealth/MassDOT to respond to the security breach and shall be fully responsible for any damages associated with the Contractor's breach including but not limited to G.L. c. 214, s. 3B.

Corporate and Business Filings and Reports. The Contractor certifies compliance with any certification, filing, reporting and service of process requirements of the Secretary of the Commonwealth, the Office of the Attorney General or other Departments as related to its conduct of business in the Commonwealth; and with its incorporating state (or foreign entity).

Employer Requirements. Contractors that are employers certify compliance with applicable state and federal employment laws or regulations, including but not limited to G.L. c. 5, s. 1 (Prevailing Wages for Printing and Distribution of Public Documents); G.L. c. 7, s. 22 (Prevailing Wages for Contracts for Meat Products and Clothing and Apparel); minimum wages and prevailing wage programs and payments; unemployment insurance and contributions; workers' compensation and insurance, child labor laws, AGO fair labor practices; G.L. c. 149 (Labor and Industries); G.L. c. 150A (Labor Relations); G.L. c. 151 and 455 CMR 2.00 (Minimum Fair Wages); G.L. c. 151A (Employment and Training); G.L. c. 151B (Unlawful Discrimination); G.L. c. 151E (Business Discrimination); G.L. c. 152 (Workers' Compensation); G.L. c.153 (Liability for Injuries); 29 USC c. 8 (Federal Fair Labor Standards); 29 USC c. 28 and the Federal Family and Medical Leave Act.

Federal And State Laws And Regulations Prohibiting Discrimination including but not limited to the Federal Equal Employment Oppurtunity (EEO) Laws the Americans with Disabilities Act.; 42 U.S.C Sec. 12,101, et seq., the Rehabilitation Act, 29 USC c. 16 s. 794; 29 USC c. 16, s. 701; 29 USC c. 14, 623; the 42 USC c. 45; (Federal Fair Housing Act); G. L. c. 151B (Unlawful Discrimination); G.L. c. 151E (Business Discrimination); the Public Accommodations Law G.L. c. 272, s. 92A; G.L. c. 272, s. 98 and 98A, Massachusetts Constitution Article CXIV and G.L. c. 93, s. 103; 47 USC c. 5, sc. II, Part II, s. 255 (Telecommunication Act; Chapter 149, Section 105D, G.L. c. 151C, G.L. c. 272, Section 92A, Section 98 and Section 98A, and G.L. c. 111, Section 199A, and Massachusetts Disability-Based Non-Discrimination Standards For Executive Branch Entities, and related Standards and Guidance, authorized under Massachusetts Executive Order or any disability-based protection arising from state or federal law or precedent. See also MCAD and MCAD links and Resources.

Small Business Purchasing Program (SBPP). A Contractor may be eligible to participate in the SBPP, created pursuant to Executive Order 523, if qualified through the SBPP COMMBUYS subscription process at: www.commbuys.com and with acceptance of the terms of the SBPP participation agreement.

Limitation of Liability for Information Technology Contracts (and other Contracts as Authorized). The Information Technology Mandatory Specifications and the IT Acquisition Accessibility Contract Language are incorporated by reference into Information Technology Contracts. The following language will apply to Information Technology contracts in the U01, U02, U03, U04, U05, U06, U07, U08, U09, U10, U75, U98 object codes in the Expenditure Classification Handbook or other Contracts as approved by CTR or OSD. Pursuant to Section 11. Indemnification of the MassDOT Terms and Conditions, the term "other damages" shall include, but shall not be limited to, the reasonable costs the Commonwealth/MassDOT incurs to repair, return, replace or seek cover (purchase of comparable substitute commodities and services) under a Contract. "Other damages" shall not include damages to the Commonwealth/MassDOT as a result of third party claims, provided, however, that the foregoing in no way limits the Commonwealth's or MassDOT's right of recovery for personal injury or property damages or patent and copyright

infringement under Section 11 nor the Commonwealth's/MassDOT's ability to join the contractor as a third party defendant. Further, the term "other damages" shall not include, and in no event shall the contractor be liable for, damages for the Commonwealth's or MassDOT's use of contractor provided products or services, loss of Commonwealth or MassDOT's records, or data (or other intangible property), loss of use of equipment, lost revenue, lost savings or lost profits of the Commonwealth or MassDOT. In no event shall "other damages" exceed the greater of $100,000, or two times the value of the product or service (as defined in the Contract scope of work) that is the subject of the claim. Section 11 sets forth the contractor's entire liability under a Contract. Nothing in this section shall limit the Commonwealth's or MassDOT's ability to negotiate higher limitations of liability in a particular Contract, provided that any such limitation must specifically reference Section 11 of the MassDOT Terms and Conditions. In the event the limitation of liability conflicts with accounting standards which mandate that there can be no cap of damages, the limitation shall be considered waived for that audit engagement. These terms may be applied to other Contracts only with prior written confirmation from the Operational Services Division or the Office of the Comptroller. The terms in this Clarification may not be modified.

Northern Ireland Certification. Pursuant to G.L. c. 7 s. 22C for state agencies, state authorities, the House of Representatives or the state Senate, by signing this Contract the Contractor certifies that it does not employ ten or more employees in an office or other facility in Northern Ireland and if the Contractor employs ten or more employees in an office or other facility located in Northern Ireland the Contractor certifies that it does not discriminate in employment, compensation, or the terms, conditions and privileges of employment on account of religious or political belief; and it promotes religious tolerance within the work place, and the eradication of any manifestations of religious and other illegal discrimination; and the Contractor is not engaged in the manufacture, distribution or sale of firearms, munitions, including rubber or plastic bullets, tear gas, armored vehicles or military aircraft for use or deployment in any activity in Northern Ireland.

Pandemic, Disaster or Emergency Performance. In the event of a serious emergency, pandemic or disaster outside the control of the Department, the Department may negotiate emergency performance from the Contractor to address the immediate needs of the MassDOTeven if not contemplated under the original Contract or procurement. Payments are subject to appropriation and other payment terms.

Consultant Contractor Certifications (For Consultant Contracts "HH" and "NN" and "U05" object codes subject to G.L. Chapter 29, s. 29A). Contractors must make required disclosures as part of the RFR Response or using the Consultant Contractor Mandatory Submission Form.

Attorneys. Attorneys or firms providing legal services or representing MassDOT may be subject to G.L. c. 30, s. 65, and if providing litigation services must be approved by the Office of the Attorney General to appear on behalf of a Department, and shall have a continuing obligation to notify the Commonwealth of any conflicts of interest arising under the Contract.

Subcontractor Performance. The Contractor certifies full responsibility for Contract performance, including subcontractors, and that comparable Contract terms will be included in subcontracts, and that the Department will not be required to directly or indirectly manage subcontractors or have any payment obligations to subcontractors. .

EXECUTIVE ORDERS

For covered Executive state Departments, the Contractor certifies compliance with applicable Executive Orders (see also Massachusetts Executive Orders), including but not limited to the specific orders listed below. A breach during period of a Contract may be considered a material breach and subject Contractor to appropriate monetary or Contract sanctions.

Executive Order 481. Prohibiting the Use of Undocumented Workers on State Contracts: For all state agencies in the Executive Branch, including all executive offices, boards, commissions, agencies, Departments, divisions, councils, bureaus, and offices, now existing and hereafter established, by signing this Contract the Contractor certifies under the pains and penalties of perjury that they shall not knowingly use undocumented workers in connection with the performance of this Contract; that, pursuant to federal requirements, shall verify the immigration status of workers assigned to a Contract without engaging in unlawful discrimination; and shall not knowingly or recklessly alter, falsify, or accept altered or falsified documents from any such worker

Executive Order 130. Anti-Boycott. The Contractor warrants, represents and agrees that during the time this Contract is in effect, neither it nor any affiliated company, as hereafter defined, participates in or cooperates with an international boycott (See IRC § 999(b)(3)-(4), and IRS Audit Guidelines Boycotts) or engages in conduct declared to be unlawful by G.L. c. 151E, s. 2. A breach in the warranty, representation, and agreement contained in this paragraph, without limiting such other rights as it may have, MassDOT and the Commonwealth shall be entitled to rescind this Contract. As used herein, an affiliated company shall be any business entity of which at least 51% of the ownership interests are directly or indirectly owned by the Contractor or by a person or persons or business entity or entities directly or indirectly owning at least 51% of the ownership interests of the Contractor, or which directly or indirectly owns at least 51% of the ownership interests of the Contractor.

Executive Order 346. Hiring of State Employees By State Contractors Contractor certifies compliance with both the conflict of interest law G.L. c. 268A specifically s. 5 (f) and this order; and includes limitations regarding the hiring of state employees by private companies contracting with the Commonwealth/MassDOT. A privatization contract shall be deemed to include a specific prohibition against the hiring at any time during the term of Contract, and for any position in the Contractor's company, any state management employee who is, was, or will be involved in the preparation of the RFP, the negotiations leading to the awarding of the Contract, the decision to award the Contract, and/or the supervision or oversight of performance under the Contract.

Executive Order 444. Disclosure of Family Relationships With Other State Employees. Each person applying for employment (including Contract work) within the Executive Branch under the Governor must disclose in writing the names of all immediate family related to immediate family by marriage who serve as employees or elected officials of the Commonwealth. All disclosures made by applicants hired by the Executive Branch under the Governor shall be made available for public inspection to the extent permissible by law by the official with whom such disclosure has been filed.

Executive Order 504. Regarding the Security and Confidentiality of Personal Information. For all Contracts involving the Contractor's access to personal information, as defined in G.L. c. 93H, and personal data, as defined in G.L. c. 66A, owned or controlled by Executive Department agencies, or access to agency systems containing such information or data (herein collectively "personal information"), Contractor certifies under the pains and penalties of perjury that the Contractor (1) has read Commonwealth of Massachusetts Executive Order 504 and agrees to protect any and all personal information; and (2) has reviewed all of the Commonwealth **Information Technology Division's Security Policies**. Notwithstanding any contractual provision to the contrary, in connection with the Contractor's performance under this Contract, for all state agencies in the Executive Department, including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices, now existing and hereafter established, the Contractor shall: (1) obtain a copy, review, and comply with the contracting agency's Information Security Program (ISP) and any pertinent security guidelines, standards, and policies; (2) comply with all of the Commonwealth of Massachusetts Information Technology Division's "Security Policies") (3) communicate and enforce the contracting agency's ISP and such Security Policies against all employees (whether such employees are direct or contracted) and subcontractors; (4) implement and maintain any other reasonable appropriate security procedures and practices necessary to protect personal information to which the Contractor is given access by the contracting agency from the unauthorized access, destruction, use, modification, disclosure or loss; (5) be responsible for the full or partial breach of any of these terms by its employees (whether such employees are direct or contracted) or subcontractors during or after the term of this Contract, and any breach of these terms may be regarded as a material breach of this Contract; (6) in the event of any unauthorized access, destruction, use, modification, disclosure or loss of the personal information (collectively referred to as the "unauthorized use"): (a) immediately notify the contracting agency if the Contractor becomes aware of the unauthorized use; (b) provide full cooperation and access to information necessary for the contracting agency to determine the scope of the unauthorized use; and (c) provide full cooperation and access to information necessary for the contracting agency and the Contractor to fulfill any notification requirements. Breach of these terms may be regarded as a material breach of this Contract, such that the Commonwealth and MassDOT may exercise any and all contractual rights and remedies, including without limitation indemnification under Section 11 of MassDOT's Terms and Conditions, withholding of payments, Contract suspension, or termination. In addition, the Contractor may be subject to applicable statutory or regulatory penalties, including and without limitation, those imposed pursuant to G.L. c. 93H and under G.L. c. 214, § 3B for violations under M.G.L c. 66A.

Executive Orders 523, 524 and 526. Executive Order 526 (Order Regarding Non-Discrimination, Diversity, Equal Opportunity and Affirmative Action which supersedes Executive Order 478). Executive Order 524 (Establishing the Massachusetts Supplier Diversity Program which supersedes Executive Order 390). Executive Order 523 (Establishing the Massachusetts Small Business Purchasing Program.) All programs, activities, and services provided, performed, licensed, chartered, funded, regulated, or contracted for by the state shall be conducted without unlawful discrimination based on race, color, age, gender, ethnicity, sexual orientation, gender identity or expression, religion, creed, ancestry, national origin, disability, veteran's status (including Vietnam-era veterans), or background. The Contractor and any subcontractors may not engage in discriminatory employment practices; and the Contractor certifies compliance with applicable federal and state laws, rules, and regulations governing fair labor and employment practices; and the Contractor commits to purchase supplies and services from certified minority or women-owned businesses, small businesses, or businesses owned by socially or economically disadvantaged persons or persons with disabilities. These provisions shall be enforced through the contracting agency, OSD, and/or the Massachusetts Commission Against Discrimination. Any breach shall be regarded as a material breach of the contract that may subject the contractor to appropriate sanctions.

Charles D. Baker, Governor
Karyn E. Polito, Lieutenant Governor
Stephanie Pollack, Secretary & CEO
Jonathan L. Gulliver, Highway Administrator

massDOT
Massachusetts Department of Transportation
Highway Division

September 3, 2020

Contract Number: 111753
Location: Statewide

Bain Cor, Inc.
763 South Street
Holbrook, MA 02343

Dear John Cordeiro,

Enclosed is a Certificate of Exemption Form ST-2 along with a Purchaser's Sales Tax Exempt Form (ST-5) for Bain Cor, Inc., which substantiates the Tax Exempt status of this Department under the provisions of Chapter 64H, s6 (d), (e), (f) or (tt). The duration of the tax forms are from July 1, 2020 until June 30, 2025.

All purchases of tangible personal property or services by this Department are exempt from taxation to the extent that such property or services are used in the conduct of the business of the purchaser.

If your contract is extended beyond the completion date on the Purchaser's Sales Tax Exempt Form (ST-5), please notify the Director of Contracts & Records for issuance of a new certificate.

Very truly yours,

Anna Dolata

Anna Dolata
Supervisor, Contracts & Records

AD/mas
Enc.
Contact: MassDOT - Planning & Enterprise Services
Ten Park Plaza – Suite 5510
Boston, MA 02116-3973
857-368-9537

Ten Park Plaza, Suite 5510, Boston, MA 02116
Tel: 857-368-9537, Fax: 857-368-0623
www.mass.gov/massdot

Commonwealth of Massachusetts
Department of Revenue
Christopher C. Harding, Commissioner

mass.gov/dor

Letter ID: L1875320960
Notice Date: March 23, 2018
MA Taxpayer ID: 10037042

CERTIFICATE OF EXEMPTION

MASSACHUSETTS DEPARTMENT OF
TRANSPORTATION
MASSDOT
10 PARK PLAZA
BOSTON MA 02116

Attached below is your Certificate of Exemption (Form ST-2). Cut along the dotted line and display at your place of business. You must report any change of name or address to us so that a revised ST-2 can be issued.

DETACH HERE

MASSACHUSETTS DEPARTMENT OF REVENUE — Form ST-2

Certificate of Exemption

MASSDOT
10 PARK PLAZA
BOSTON MA 02116

MA Taxpayer ID: 10037042
Certificate Number: 1310988288

This certifies that the organization named above is an exempt purchaser under Chapter 64H, section 6(d) or (e) of the Massachusetts General Laws. All purchases of tangible personal property by this organization are exempt from taxation to the extent that such property is used in the conduct of the business of the purchaser. Misuse of this certificate by any tax-exempt organization or unauthorized use of this certificate by any individual will lead to revocation. Willful misuse of this certificate is subject to criminal sanctions of up to one year in prison and $10,000 ($50,000 for corporations) in fines. This certificate is non-transferable and may be suspended or revoked for failure to comply with state laws and regulations.

Effective Date: March 23, 2018

Expiration Date: March 22, 2028

Form ST-5
Sales Tax Exempt Purchaser Certificate

Rev. 6/09
919
Massachusetts Department of Revenue

Part 1. Exempt taxpayer information. To be completed by exempt government or 501(c)(3) organization.

Name
Massachusetts Department of Transportation - Highway Division

Address
10 Park Plaza

City | State | Zip
Boston, MA 02116

Exemption number
04-6002284

Issue date | Date of expiration of certificate
July 1, 2020 | June 30, 2025

Certification is hereby made that the organization named above is an exempt purchaser under Massachusetts General Laws, Chapter 64H, sections 6(d) or 6(e). All purchases of tangible personal property or services by this organization are exempt from taxation under said chapter to the extent that such property or services are used in the conduct of the business of the purchaser. Any abuse or misuse of this certificate by any tax-exempt organization or any unauthorized use of this certificate by any individual constitutes a serious violation and will lead to revocation.

Signature *Anna Dolata* | Title: Director of Contracts & Records | Date: September 3, 2020

Warning: Willful misuse of this certificate may result in criminal tax evasion sanctions of up to one year in prison and $10,000 ($50,000 for corporations) in fines.

Part 2. Agent information. To be completed by agent of exempt government or 501(c)(3) organization.

Name of agent's organization
Bain Cor, Inc. (MassDOT Contract # 111753)

Address
763 South Street

City | State | Zip
Holbrook, MA 02343

Agent's name

Address

City | State | Zip

I certify that in making this purchase, I am acting as an agent for the exempt organization named above (select one):

☑ Government organization (local public school, city/town government, state agency, etc.).
Attach Form ST-2, if available. If Form ST-2 is not available, enter exemption number, if known:

☐ 501(c)(3) organization (parochial school, Scout troop, etc.). Form ST-2 must be attached.

Signature | Title | Date

Part 3. Vendor information

Vendor's name: Bain Cor, Inc.

Check applicable box:

☐ Single purchase certificate (attach detailed receipts or complete Part 4, on reverse)

☑ Blanket certificate

This form is approved by the Commissioner of Revenue and may be reproduced.

Part 4. Description of property purchased

Date	Description	Quantity	Cost
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
		Total cost	$

General information

An exempt 501(c)(3) organization must have obtained a Certificate of Exemption (Form ST-2) from the Commissioner of Revenue certifying that it is entitled to exemption under G.L. c.64H, §6(e). The 501(c)(3) organization must submit to the vendor a properly completed Sales Tax Exempt Purchaser Certificate (Form ST-5) signed by the 501(c)(3) organization with a copy of its Form ST-2 attached.

Any person, group or organization purchasing as an agent on behalf of a 501(c)(3) organization must certify that it is doing so by presenting to the vendor a properly completed Form ST-5 signed by the 501(c)(3) organization. It must also present a copy of the 501(c)(3) organization's Form ST-2. The agent of the exempt 501(c)(3) organization must complete Part 2 of Form ST-5.

Any government organization is encouraged to obtain a Certificate of Exemption (Form ST-2) from the Commissioner of Revenue, certifying that it is entitled to exemption under G.L. c.64, § 6(d). The exempt government organization is encouraged to submit to the vendor a properly completed Sales Tax Exempt Purchaser Certificate (Form ST-5) with a copy of its Form ST-2 attached. If the government organization does not present Form ST-5, the vendor must maintain adequate documentation (generally, a copy of the government check) verifying that the purchaser is an exempt government agency.

Any person, group or organization purchasing on behalf of exempt government organizations must certify that they are doing so by presenting to the vendor a properly executed Form ST-5 when making such purchases. Part 1 of Form ST-5 should be filled out by the exempt government organization. If Part 1 is not completed by the exempt government organization, the agent must enter the name, address, and, if available, the exemption number of the government organization on whose behalf the purchases are being made. Also enter a description of the property purchased into Part 4. The agent must complete Part 2 when acting on behalf of the exempt government organization. The purchaser must attach to the Form ST-5 a copy of the exempt government organization's Form ST-2 if available. If it is not available, the purchaser must enter the exemption number of the exempt government organization.

Other information for vendors

Vendors should verify the validity of the certificate presented to them by checking the expiration date on the certificate. Vendors must **not** honor a Certificate of Exemption that has expired.

Government organization maintain Form ST-2 Certificates of Exemption that have an expiration date of "None."

Vendors should call the Customer Service Bureau at (617) 887-6367 if they have any questions regarding a Certificate of Exemption which is presented to them.

If you have any questions about completing this certificate, please contact: **Massachusetts Department of Revenue, Customer Service Bureau, 200 Arlington Street, Chelsea, MA 02150; (617) 887-6367.**

Charles D. Baker, Governor
Karyn E. Polito, Lieutenant Governor
Stephanie Pollack, Secretary & CEO
Jonathan L. Gulliver, Highway Administrator

MassDOT
Massachusetts Department of Transportation
Highway Division

INTEROFFICE MEMORANDUM

TO: MA Comptroller Office

FROM: Christine Hurley-Barnes

DATE: August 20, 2020

RE: Contract # 111753, Bain Cor Inc

SUBJECT: Standard Contract – Anticipated Start Date

The attached signed MassDOT Standard Contract form includes an anticipated start date of July 1, 2020 which was prior to the effective date of August 20, 2020 for the contract award (Contract #111753.)

Due to delays in the execution of this award, this contract needed to proceed prior to the Effective Date of the contract to ensure continuity of contract service. There are no known obligations incurred from July 1, 2020 to August 20, 2020.

Ten Park Plaza, Suite 4160, Boston, MA 02116
Tel: 857-368-4636, TTY: 857-368-0655
www.mass.gov/massdot

COMMONWEALTH OF MASSACHUSETTS
Prompt Pay Discount Form
(Invoice discounts for receiving fast payments)

Revised 3/9/07

Bidder Name: Bain Cor
Vendor Code (VCUST): VC0000506451
Contract/RFR Number(s): 99522 111753

Prompt Payment Discounts (PPD). All contractors/vendors doing business with the Commonwealth must provide a Prompt Payment Discount (PPD) for receiving early payments unless the Contractor/vendor can provide compelling proof that providing a prompt pay discount would be unduly burdensome. Contractors benefit from PPD by increased, usable cash flow as a result of fast and efficient payments for commodities or services rendered. Contractors who agree to accept Electronic Funds Transfer (EFT) increase the prompt pay benefit by ensuring that funds are paid directly to their designated bank accounts, thus eliminating the delay of check clearance policies and traditional mail lead time. Payments processed through the state accounting system (MMARS) can be tracked and verified through the Comptroller's Vendor Web system using the Vendor/Customer Code assigned to you by a Commonwealth department.

The Commonwealth benefits because contractors reduce the cost of products and services through the applied discount. While Bidders/Contractors have flexibility in determining the actual % discount(s) offered to the Commonwealth, the discount(s) must be identified for 10, 15, 20 and/or 30 days for payment issuance in the column entitled "% Discount Off Proposed Price" below. The Commonwealth may use the prompt pay discounts submitted as a basis for selection and may negotiate discounts as deemed in the best interest of the Commonwealth. The requirement to offer PPD discounts may be waived by the Commonwealth on a case-by-case basis if participation in the program would be unduly burdensome, provided the specific reason for the hardship is outlined below.

All discounts offered will be taken in cases where the payment issue date is within the specified number of days listed below and in accordance with the Commonwealth's Bill Paying Policy. Payment days will be measured **from** the date goods are received and accepted / performance was completed OR the date an invoice is received by the Commonwealth, whichever is later **to** the date the payment is issued as an EFT (preferred method) or mailed by the State Treasurer. The date of payment "issue" is the date a payment is considered "paid" not the date a payment is "received" by a Contractor.

If internal Bidder/Contractor systems require an alternate method of measuring payment issue dates, the Bidder/Contractor must note the issues below or on an attached page if necessary to be considered by the PMT. In cases where the Bidder/Contractor considers that offering a Prompt Payment Discount would be a hardship, the Bidder must clearly define the issues and reasons for said hardship. *Providing volume discounts or other discounts on prices is not considered a hardship, since the PPD provides the additional benefit of early cash flow for the Contractor.*

Enter the Prompt Payment Discount percentage (%) off the invoice payment, for each of the payment issue dates listed, if the payment is issued within the specified Payment Issue days. For example:

5% - 10 Days
4% - 15 Days
3% - 20 Days
2% - 30 Days

If no discount is offered enter 0%

Prompt Payment Discount %	Payment Issue Date w/in
2 %	10 Days
%	15 Days
%	20 Days
%	30 Days

The Contractor is unable to provide a prompt payment discount due to the following hardship:

Contractor/Bidder Authorized Signature John Cordeiro
Date: 4/7/2020

Contractor/ Bidder Authorized Signatory Print Name and Title: Vice President

BIDDER CURRENT ENVIRONMENTALLY PREFERABLE PRODUCTS / PRACTICES FORM

Bidder Company Name: Bain Coe Inc Date: 4/9/20

This form is a standard evaluation tool. Questions 1- 6 apply to the operations of the Bidder (not the operations of a manufacturer or other company the bidder works with). Question 7 requests additional information about environmentally preferable product offerings.

The primary purpose of this form is to encourage potential Bidders to communicate existing business practices that foster a sustainable approach to conducting their operations. This may include one that has a reduced impact on the environment or public health, such as, but not limited to, creating less waste by using less packaging; eliminating the use substances and/or materials that are considered toxic; or using alternative fuel vehicles in the delivery fleet for the purpose of reducing air pollution and greenhouse gas emissions.

The Commonwealth considers such initiatives part of the "best value" of procurement. **Bidders have an opportunity to receive additional points in the evaluation phase of the RFR for the environmental initiatives they have identified.** However, bidders must substantiate all answers in the space provided below or in an attachment in order to receive any additional points. If reference is made to an attached document, or a website, list the specific page and line to which information is referenced.

1. **Sustainability Program/Environmental Business Practices**
   a) Does your firm have a corporate-wide sustainability policy? If yes, attach or provide a link to your sustainability policy AND summarize what your corporate sustainability policy directs your company to do: Click here to enter text.

   b) Indicate any other types of corporate sustainability policies AND attach policy in order to receive credit.
   ☐Climate Action Plan
   ☐Zero Waste Policy
   ☐Toxics Reduction Strategy
   ☐Green Fleet Policy
   ☐Sustainable Procurement Policy or Environmentally Preferable Purchasing Policy
   ☑Waste Prevention and/or recycling policy/program (describe and list types of materials you recycle) CARD BOARD BOXES, SHIPPING MATERIAL

   Briefly describe and list sustainable procurement practices and achievements as a result of the policies checked above: Click here to enter text.

   c) Does your company publish an annual Sustainability Report listing accomplishments and future goals? If yes, please attach (or provide a link to) your latest Sustainability Report. Please describe key elements and accomplishments (such as receiving sustainability awards). Click here to enter text.

   d) Please list individual steps not indicated above that your firm has taken to improve the sustainability at your own operations:
   ☐ Uses at least 50% remanufactured toner cartridges in printers (attach total annual spend on remanufactured and Original Equipment Manufacturer cartridges) Click here to enter text.
   ☐ Uses Green Cleaning products (certified by UL Ecologo, GreenSeal or SaferChoice) in all cleaning or janitorial services (attach copy of scope of work with cleaning services provider and types of green products used) Click here to enter text.

- ☐ Purchase appliances and equipment (printers, copiers, microwaves, etc.), that are Energy Star or EPEAT certified models. (list certified products) Click here to enter text.
- ☐ Incorporates green building design elements into all construction and renovation projects (list green design elements and provide documentation). Click here to enter text.
- ☐ Owns or leases buildings certified to LEED or another green building standard? (describe) Click here to enter text.
- ☐ Purchases or creates renewable electricity onsite (through solar or wind systems, for example)? Describe and indicate the % of energy that is derived from renewable sources: Click here to enter text.
- ☐ Has received a third party energy audit (usually through the utility) and implemented recommendations (attach audit recommendations and identify what has been completed). Click here to enter text.
- ☐ Has received a third party waste audit and implemented recommendations (attach audit recommendations and identify what has been completed). Click here to enter text.
- ☐ Please list other sustainable initiatives (e.g., waste reduction programs, green building management programs, other energy efficiency programs, etc.) and provide any measurable data: Click here to enter text.

2. **Packaging**:

Has your company implemented any of the following environmental packaging initiatives?

- ☑ All packaging contains post-consumer recycled materials. List post-consumer recycled content: Click here to enter text. BOXES, WRAP, Stuffed Paper and Styrofoam
- ☐ Eliminates the use (or reduces the size) of disposable containers (e.g., uses reusable shipping containers). Please describe: Click here to enter text.
- ☐ Packaging materials do not contain chemicals or materials of concern such as PVC (vinyl), BPA, etc.). Please describe: Click here to enter text.

3. **Shipping/Transportation:**

Describe in detail how your company has implemented environmentally sound shipping and transportation practices.

- ☐ Your firm uses electric, hybrid-electric, bicycles or other alternative fuel vehicles to transport products to your retail stores or other locations. (Describe program) Click here to enter text.
- ☐ Your firm is a US EPA SmartWay Partner. Attach partnership agreement. Click here to enter text.
- ☐ Has an anti-idling policy. Attach policy.
- ☐ Diesel vehicles are equipped with emission control devices. List device(s) here: Click here to enter text.
- ☐ Uses biodiesel in your vehicles. List estimated amount used in the last year: Click here to enter text.
- ☐ Use environmentally preferable products in its fleet program (e.g., retread tires, re-refined motor oil, low-VOC solvents, etc.). List products here: Click here to enter text.
- ☐ Encourages the use of public/green transit. Provide name and description of program(s): Click here to enter text.
- ☐ Minimizes shipping energy and environmental impacts in other ways? Please describe: Click here to enter text.

4. **Training and Education**

Describe how your company trains staff and educates customers on the products or service that involves an environmentally preferable component. Click here to enter text.

5. **Certifications**

Bidders should familiarize themselves with the various certifications for products and processes that are available within the industry in which they operate, with particular attention to those concerning environmental issues. Has your company or any of its manufacturers and/or subcontractors obtained any of the following product / industry certifications? In order to receive credit, please attach a copy certifications listed below:

- ☐ Is a reporting member of the WasteWise Program (EPA and Massachusetts) (attach most recent reporting).
- ☐ Has adopted an environmental management system that is geared to continuous improvement (e.g., ISO 14000) (attach copy of summary EMS audit).
- ☐ Certified as a Massachusetts Sustainable Business Leader through the Sustainable Business Leader Program (attach certification). Click here to enter text.
- ☐ Other industry environmental standards (where applicable), such as the CERES principles, LEED Certification, C2C Protocol, Responsible Care Codes of Practice or other similar standards (list standard) Click here to enter text.
- ☐ Other. Please describe: Click here to enter text.

6. **Other Environmental Criteria**

Bidders may provide additional information about environmentally preferable practices that are not indicated and explained above (attach any appropriate documentation to substantiate claim)
Click here to enter text.

7. **Environmental Product Offering:**

Bidders providing environmentally preferable options in the price sheet should also provide additional information about those options here. Please include a description of the product, how the product is environmentally preferable, how pricing compares to the conventional product counterpart, links to additional information, or if attaching product information, please reference names of files, and any additional information that would be helpful for reviewer:
Click here to enter text.

Supplier Diversity Program (SDP) Plan Commitment
SDP Plan Form #1

Contract/RFR Document Number: Click here to enter text.

Instructions: Completing all parts of this form is mandatory. Please read all sections of the Bid related to the SDP. Complete one form and submit with your Quote.

Important: Prime bidders that are certified as an M/WBE, M/WNPO, VBE, SDVOBE, DOBE and LGBTBE must also submit an SDP Plan Form and may not list themselves or their affiliates as SDP Partners.

Part I Bidder/Contractor Information (Required)			
Business Name: Bain Cor Inc	**Contact Name: John Cordeiro.**	**Phone #**: 339-987-5525.	**Email address**: 763 South St STE A Holbrook MA 02343

Part II Annual Financial Commitment (Required)	
Provide a specific percentage of Bidder/Contractor sales derived from this contract to be spent with all certified SDP Partners on a Massachusetts fiscal year (July 1-June 30) basis.	
Annual SDP Percentage Committed in Bid Response for Life of Contract:	**.05.%**

Supplier Diversity Program (SDP) Resources:

- Lists of M/WBEs, M/WNPOs, VBEs, SDVOBEs, DOBEs and LGBTBEs certified or verified by the Supplier Diversity Office (SDO) are located at www.mass.gov/sdo.
- Resources to assist Prime Bidders in finding potential Certified Partners can be found at www.mass.gov/sdp.

Corporations Division

Business Entity Summary

ID Number: 270560321 Request certificate New search

Summary for: BAIN COR, INC.

The exact name of the Domestic Profit Corporation: BAIN COR, INC.	
Entity type: Domestic Profit Corporation	
Identification Number: 270560321	**Old ID Number:** 001008315
Date of Organization in Massachusetts: 07-21-2009	
	Last date certain:
Current Fiscal Month/Day: 12/31	**Previous Fiscal Month/Day:** 12/31

The location of the Principal Office:

Address: 763 SOUTH STREET

City or town, State, Zip code, Country: HOLBRROK, MA 02343 USA

The name and address of the Registered Agent:

Name: WAYNE BAINTER

Address: 763 SOUTH STREET

City or town, State, Zip code, Country: HOLBROOK, MA 02343 USA

The Officers and Directors of the Corporation:

Title	Individual Name	Address
PRESIDENT	WAYNE BAINTER	763 SOUTH STREET HOLBROOK, MA 02343 USA
PRESIDENT	WAYNE BAINTER	763 SOUTH STREET, SUITE A HOLBROOK, MA 02343 USA
TREASURER	JOHN A. CORDEIRO	763 SOUTH STREET, SUITE A HOLBROOK, MA 02343 USA
SECRETARY	WAYNE BAINTER	763 SOUTH STREET, SUITE A HOLBROOK, MA 02343 USA
VICE PRESIDENT	JOHN A. CORDEIRO	763 SOUTH STREET, SUITE A HOLBROOK, MA 02343 USA
DIRECTOR	WAYNE BAINTER	763 SOUTH STREET, SUITE A HOLBROOK, MA 02343 USA
DIRECTOR	JOHN A. CORDEIRO	763 SOUTH STREET, SUITE A HOLBROOK, MA 02343 USA

Business entity stock is publicly traded:

The total number of shares and the par value, if any, of each class of stock which this business entity is authorized to issue:

ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 04/09/20

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME: Sue Purdy	
East Bridgewater Insurance Agency 76 North Bedford Street East Bridgewater, MA 02333	PHONE (A/C, No, Ext): 508-378-3991	FAX (A/C, No): 508-378-9558
	E-MAIL ADDRESS: sjpurdy@ebinsuranceinc.com	
	INSURER(S) AFFORDING COVERAGE	NAIC #
	INSURER A : Arbella Protection	
INSURED Baincor Inc. 763 South Street Holbrook, MA	INSURER B :	
	INSURER C :	
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	[X] COMMERCIAL GENERAL LIABILITY [ ] CLAIMS-MADE [X] OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: [X] POLICY [ ] PRO-JECT [ ] LOC [ ] OTHER:			8500064514	07/08/19	07/08/20	EACH OCCURRENCE	$ 1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 100,000
							MED EXP (Any one person)	$ 5,000
							PERSONAL & ADV INJURY	$ 1,000,000
							GENERAL AGGREGATE	$ 2,000,000
							PRODUCTS - COMP/OP AGG	$ 2,000,000
								$
A	AUTOMOBILE LIABILITY [X] ANY AUTO [ ] OWNED AUTOS ONLY [ ] SCHEDULED AUTOS [ ] HIRED AUTOS ONLY [ ] NON-OWNED AUTOS ONLY			1020043132	06/29/19	06/29/20	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
	[ ] UMBRELLA LIAB [ ] OCCUR [ ] EXCESS LIAB [ ] CLAIMS-MADE [ ] DED [ ] RETENTION $						EACH OCCURRENCE	$
							AGGREGATE	$
								$
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N [ ] If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		4220055617	07/08/19	07/08/20	[X] PER STATUTE [ ] OTH-ER	
							E.L. EACH ACCIDENT	$ 1,000,000
							E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

Proof of Insurance

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Peter Spagone, Jr.

© 1988-2015 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD

BUSINESS REFERENCE FORM

Bidder: Bain Cor Inc

RFR Name/Title: Equipment, Parts & Services for Telecommunications, ITS, IRS Systems

RFR Number: BD-20-1030-01100-60070-49476

The bidder must provide (indicate a number) 3 business references.

Reference name: AETNA BRIDGE COMPANY Contact: KEN LANAGAN

Address: 200 BABCOCK RD CRANSTON RI Phone: # (401) 295-0336

Fax/Internet address: 401 295-0307 KLANAGAN@AETNABRIDGE.COM

Description and date(s) of commodities and services provided: Sales and Service of truck mounted attenuators, Message Boards Arrow Boards Ground mounted Attenuators temp Barrier, speed Radars trailers and all Traffic Safety Products.

Reference name: RHODE ISLAND DEPT. of TRANS Contact: Alexander R. PACHECO

Address: 360 Lincoln AVE Phone: # (401) 734 4872

Fax/Internet address: 401 736 0196 alex.pacheco@dot.ri.gov

Description and date(s) of commodities and services provided: Sales and Service OF Truck mounted Attenuators trailer attenuators, Message Boards, Arrow Boards Trailer and truck mounted and repairs of traffic safety products.

Reference name: MASSDOT Contact: Frank Hawe

Address: Lexington Depot Phone: # ( )

Fax/Internet address: Frank.Hawe@state.ma.us

Description and date(s) of commodities and services provided: Sales + Service of truck mounted and trailer Attenuators, service light towers, message Boards Arrow Boards mounted and trailers. Service all traffic safety Products.

References will be contacted to confirm the bidder's abilities and qualifications as stated in the bidder's response. The department may deem the bidder's response unresponsive if a reference is not obtainable from a listed reference after reasonable attempts.

Sensitivity level - low

Department Of Transportation

MASTER AGREEMENT

DOCUMENT I.D.			Document Name	
CODE	DEPT	UNIT	DOCUMENT IDENTIFIER	ACTION
MA	DOT	0701	INTF0000K03C00111753	entry

Budget FY:	2021	Document Description:	Equipment, Parts & Services for MassDOT's Telecommunications, ITS, IPCS			Vendor Ln:			
Fiscal Year:	2021	Board Award Number:	MDOTWESTON035	VC Number:	VC0000506451				
Period:	2	Authorized Department:	DOT	Addrss Code:	AD001				
Requester ID:	dotavw	MA Effective Date:	07/01/2020	Vendor Name:	BAIN COR INC				
Requester Name:	Christine Hurley Barnes	MA Expiration Date:	06/30/2025	Street Address:	763 South St				
			City:	Holbrook	State:	MA	Zip Cd:	02343	

COMMODITY INFORMATION

Commodity Ln:

Commodity Code:	432000000000	Catalog: None Provided (if none)	none provided		Commodity Specs:	Equipment, Parts & Services for MassDot's Telecommunications, ITS, IPCS
Line Type:	discount				Extended Discription:	
Unit of Measurement:	ea	Discount From: mm/dd/yyyy	07/01/2020	Service From: mm/dd/yyyy	07/01/2020	
Unit Price:	$0.00	Discount To: mm/dd/yyyy	06/30/2025	Service To: mm/dd/yyyy	06/30/2025	

Commodity Ln:

Commodity Code:	731521000000	Catalog: None Provided (if none)	none provided		Commodity Specs:	Service Support / consult / eng. Of Telecomm, ITS, IPCS systems
Line Type:					Extended Discription:	Service Support / consult / eng. Of Telecomm, ITS, IPCS systems
Unit of Measurement:		Discount From: mm/dd/yyyy	04/05/2016	Service From: mm/dd/yyyy	04/05/2016	
Unit Price:		Discount To: mm/dd/yyyy	04/04/2020	Service To: mm/dd/yyyy	04/04/2020	

TO THE COMPTROLLER OF THE COMMONWEALTH OF MASSACHUSETTS

I hereby certify under the penalties of perjury that all laws of the Commonwealth governing disbursements of public funds and the regulations therof have been complied with and observed.

SIGNED: Sharon Rong — Prepared by — TITLE: BMS — DATE: 8/7/2020

SIGNED: christine hurley barnes — Digitally signed by christine hurley barnes Date: 2020.08.10 14:41:39 -04'00' — Authorized Signatory — TITLE: — DATE:

FOR FISCAL USE ONLY

Entered By:_____ Date_____ (Initial)

Verified By:_____ Date_____ (Initial)

Issued May 2004

Massachusetts Department of Transportation
CONTRACTOR AUTHORIZED SIGNATORY LISTING

CONTRACTOR LEGAL NAME: Bain Cor, Inc.
CONTRACTOR VENDOR/CUSTOMER CODE: VC 0000506451

INSTRUCTIONS: Any Contractor (other than a sole-proprietor or an individual contractor) must provide a listing of individuals who are authorized as legal representatives of the Contractor who can sign contracts and other legally binding documents related to the contract on the Contractor's behalf. In addition to this listing, any state department may require additional proof of authority to sign contracts on behalf of the Contractor, or proof of authenticity of signature (a notarized signature that the Department can use to verify that the signature and date that appear on the Contract or other legal document was actually made by the Contractor's authorized signatory, and not by a representative, designee or other individual.)

NOTICE: ***Acceptance of any payment under a Contract or Grant shall operate as a waiver of any defense by the Contractor challenging the existence of a valid Contract due to an alleged lack of actual authority to execute the document by the signatory.***

For privacy purposes **DO NOT ATTACH** any documentation containing personal information, such as bank account numbers, social security numbers, driver's licenses, home addresses, social security cards or any other personally identifiable information that you do not want released as part of a public record. The Commonwealth reserves the right to publish the names and titles of authorized signatories of contractors.

AUTHORIZED SIGNATORY NAME	TITLE
Wayne Bainter	President
John Cordeiro	Vice President

I certify that I am the President, Chief Executive Officer, Chief Fiscal Officer, Corporate Clerk or Legal Counsel for the Contractor and as an authorized officer of the Contractor I certify that the names of the individuals identified on this listing are current as of the date of execution below and that these individuals are authorized to sign contracts and other legally binding documents related to contracts with the Commonwealth of Massachusetts on behalf of the Contractor. I understand and agree that the Contractor has a duty to ensure that this listing is immediately updated and communicated to any state department with which the Contractor does business whenever the authorized signatories above retire, are otherwise terminated from the Contractor's employ, have their responsibilities changed resulting in their no longer being authorized to sign contracts with the Commonwealth or whenever new signatories are designated.

John Cordeiro
Signature

Date: 4/9/2020

Title: Vice President

Telephone: 339-987-5525

Fax: 339-987-5528

Email: jcordeiro@baincor.com

[Listing can not be accepted without all of this information completed.]

A copy of this listing must be attached to the "record copy" of a contract filed with the department.

Massachusetts Department of Transportation
CONTRACTOR AUTHORIZED SIGNATORY LISTING

CONTRACTOR LEGAL NAME: Bain Cor, Inc.
CONTRACTOR VENDOR/CUSTOMER CODE: VC0000506451

PROOF OF AUTHENTICATION OF SIGNATURE

It is a requirement of MassDOT to obtain authentication of signatures for all signatories listed on the attached Contractor Authorized Listing

This Section MUST be completed by the Contractor Authorized Signatory in presence of notary.

Signatory's full legal name (print or type): JOHN CORDEIRO

Title: Vice President

X John Cordeiro

Signature as it will appear on contract or other document **(Complete only in presence of notary):**

AUTHENTICATED BY NOTARY OR CORPORATE CLERK (PICK ONLY ONE) AS FOLLOWS:

I, Brian T McNeil (NOTARY) as a notary public certify that I witnessed the signature of the aforementioned signatory above and I verified the individual's identity on this date:

March 19, 20 20.

My commission expires on: 11-08-24

BRIAN T MCNEIL
Notary Public
Commonwealth of Massachusetts
My Commission Expires

AFFIX NOTARY SEAL

I, Wayne Bain (CORPORATE CLERK) certify that I witnessed the signature of the aforementioned signatory above, that I verified the individual's identity and confirm the individual's authority as an authorized signatory for the Contractor on this date:

3-19, 20 20.

AFFIX CORPORATE SEAL

Chorus Intelligence Suite

Discover • Link • Solve



Chorus

Empowerment Through Data



Law enforcement at a glance

The volume of digital data is growing and it is difficult to access, analyze, store and share. Law enforcement agencies are under immense pressure to leverage and control their digital data and stay ahead of the curve in tackling crime.

However, the strain on resources has never been more acute. Crime rates are rising and much of this can be attributed to digitally enabled crime, which is becoming ever more prevalent.

Agencies of all shapes and sizes are not equipped with the right tools to manage and leverage data to its full potential, which is why we created the Chorus Intelligence Suite (CIS).

Cloud-based and modular, the CIS equips anyone involved in digital investigations with the tools to self-serve and confidently turn data into intelligence and evidence.



One intelligence platform to empower your entire organization to tackle:

- Serious and organized crime
- Violent crime
- Domestic crime
- Gang-led crime
- Mass gatherings/civil unrest
- School safety issues
- Gun crime
- Human trafficking

Realize the full potential of your data

Analysts, Investigators, open-source experts and front-line officers are all empowered to carry out digital investigations through our intuitive and fully integrated software platform. Key capabilities include:

Save time
Conduct digital investigations from one intelligence platform

Empower multiple roles
Enable investigators and front-line officers to easily get answers from their data

Enrich evidence
Cleanse, combine and connect data to spot connections

Power up OSINT investigations
Search across 180+ data connectors & perform federated searches

Increase collaboration
Share intelligence with colleagues, partners and external organizations

Safe and secure
A Software as a Service (SaaS), platform, which protects your anonymity

The Chorus Intelligence Suite

Be empowered at every stage of a digital investigation to realize the full potential of your data.

A single data and case store

The CIS is a digital repository for all digital data related to an investigation. Browser-based, it can be securely accessed at any time.

FIND OUT MORE

Federated OSINT and consented data search

Perform federated searches across multiple social media and consented data sources alongside unstructured data held locally by your organization, from one user interface. Combine intelligence from multiple sources.

FIND OUT MORE

Internal data ingestion

In addition to leveraging OSINT and consented data, Chorus can tailor specific integrations to each organization where the requirement exists e.g. CAD/RMS and a plethora of other line of business systems.

FIND OUT MORE

Unstructured data upload

Uncover hidden intelligence across your disparate, internal, and legacy unstructured data. The CIS allows you to upload this, index it and make it searchable.

FIND OUT MORE

Cleanse, combine and connect analytical data

Use an intuitive and customizable dashboard to overlay different data types to identify patterns, make connections and answer key questions.

FIND OUT MORE

Security assurance

The CIS is a platform with security at its core. Deploy it using the AWS Government Cloud, built in line with CJIS standards.

FIND OUT MORE

A single data and case store

Combine and connect all digital data sources and store in one single location. Spot connections and share with colleagues, partners, and external agencies:

Key capabilities include:

- **Fully searchable content** - Any data that is captured or sourced across the CIS can be indexed and searched.
- **Bulk search data for cross-case analysis** – All content in the CIS is fully searchable and allows you to instantly bulk search data to reveal cross overs. Unlock intelligence held in your existing Chorus data, within both historical and operational files, and perform cross-case analysis to aid investigations.
- **Maintain a bird's eye view of activity** - View a timeline of when any searches, web captures, and activities are performed, by who and when.

  Automatic and manual redaction- The CIS recognizes keywords, telephone numbers or names from captured web pages. You can automatically or manually redact a file.
- **Extensive reporting suite -** Generate reports from all the data and intelligence that you have stored. This includes association charts, websites, social media pages, videos, and maps.



Store and share digital intelligence

Federated OSINT and consented data search

Bulk search across 180+ social media networks

Use the CIS to perform federated searches across multiple social media data sources, consented data sources and unstructured data held locally by your organization, to compare information.

This approach not only improves the effectiveness of data capture, it gives analysts, investigators and front line officers the best possible chance of finding key information about a subject or entity.

Overlay, analyze and compare this widely distributed data in multiple ways, to spot connections and prioritize what is important to your investigation.



"Evidence has now gone digital. We must get a grip on the vast tide of criminal data and find a way to use it to our advantage. Having one tool that helps us analyze this digital evidence and find answers makes a huge difference.

- Major Crime Investigator

OSINT Powered up by

SHADOWDRAGON

Key features include:

- **Bulk search across 180+ social media networks –** Including Facebook, Instagram, Twitter, LinkedIn, Snapchat, TikTok, Telegram, eBay, Cash App, YouTube, WhatsApp, TruthSocial and many more.
- **Search hashtags –** For people, places, upcoming events, mass gatherings or any search terms related to your investigation.
- **Go anonymous –** Embed and capture intelligence from your own undercover social media accounts in a discrete, secure and audited environment.
- **Auto-matching –** Identify data in one case that has been previously captured in another.

Key benefits include:

- **Never miss a connection -** Leave no stone unturned. Customize your connectors and bulk search across them to reveal unknown intelligence.
- **Enrich your investigations -** Expand your data sets and visualize in multiple ways to spot patterns.
- **Get the full picture -** Merge OSINT results with other data sources to aid the attribution process.
- **Stay ahead of the game –** Ensure that key new information is captured immediately via watchlist alerts.
- **Minimize risk –** Leverage hashtag searches to monitor emerging threats and/or for public safety planning purposes to determine appropriate resource allocation.



Bulk search 180+ social media networks

Untap the potential of your unstructured and internal data

Uncover hidden intelligence across your disparate, internal, and legacy data

When it comes to gathering intelligence for a case, law enforcement agencies will often have masses of useful digital data hidden in unstructured and disparate legacy files.

Make your legacy data searchable

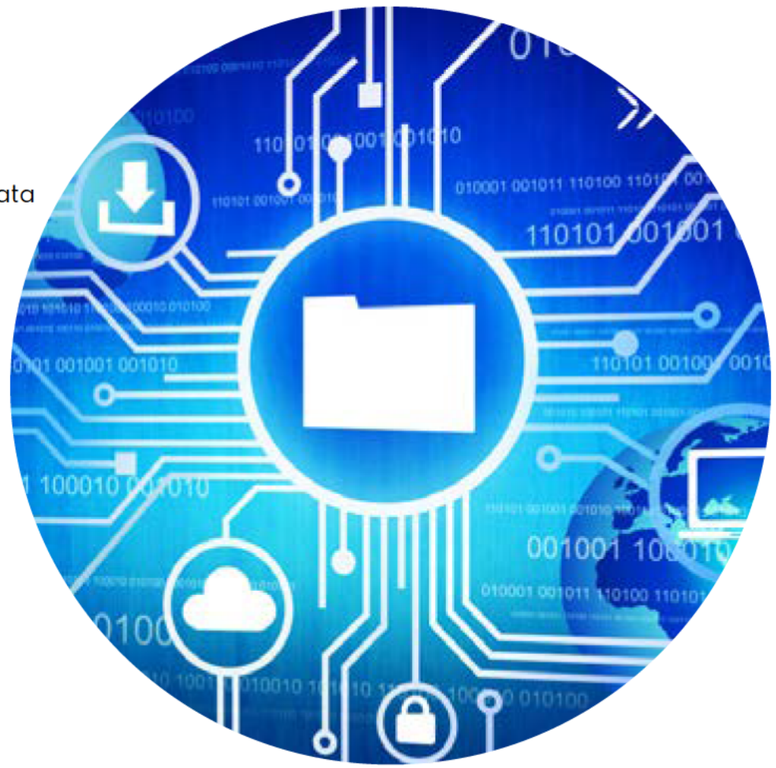
Use the CIS to upload unstructured data files via a secure upload portal.

The CIS enables users to index and search this data ensuring that hidden and historic intelligence is made use of.

The CIS supports an extensive range of file types including image-based PDFs that are fully searchable.

Internal data interfaces

In addition to leveraging OSINT, consented data and unstructured data, Chorus can tailor specific integrations to each organization where the requirement exists e.g. Record Management Systems (RMS), Jail Management Systems (JMS), and a plethora of other line of business systems.



Cleanse, combine and connect your analytical data

Empower Investigators and front-line officers to get answers from digital data

With police departments under more pressure than ever to speed up investigations and secure convictions, having the means to democratize data analysis and alleviate the reliance on skilled analysts to investigate crimes has become a necessity.

The CIS features an intuitive dashboard capability that empowers investigators and front line officers to get answers from their data, immediately. Users can simply ingest data and take advantage of automated cleansing rules to work out the who, what, where and when of a digital investigation. Data types leveraged can include:

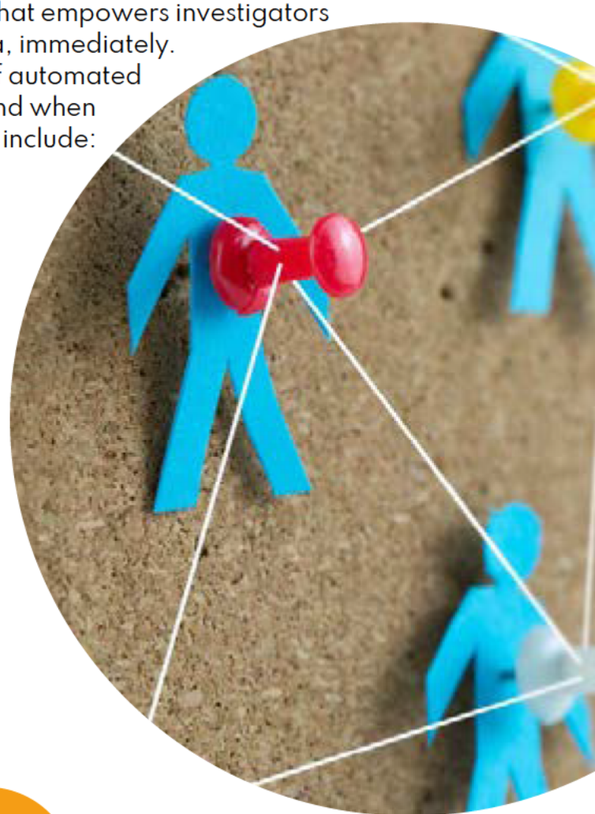
- Communications data (call data records)
- Handset downloads
- RF surveys
- ALPR
- Bank statements
- Chat, instant messaging and more

Visualize, enrich, and expand

Overlay these different data types to identify patterns, make connections and answer key investigative questions. Produce maps, timelines, event schedules and charts.

Customized reporting

Query the most frequently asked investigative questions and generate reports, to be used as potential evidence. For example, report on a suspect's top 10 interactions or identify potential meetings between individuals.



97% time saving

Cloud-based and modular deployment



Security assured

The CIS is a platform with security at its core. You can deploy it using the AWS Government Cloud, built in line with CJIS standards. Benefits include:

- **Full obfuscation** - Protect your anonymity whilst conducting online investigation searches in a fully obfuscated environment. Data is encrypted at rest and in transit.
- **Controlled user permissions -** Access to the CIS and the data within it is user permission controlled, from read-only through to full administration rights.
- **Audit logs** - Maintain comprehensive audit logs to see who has accessed what and when and also document the evidential chain of custody.

We do not own or access your data

The CIS allows users to search multiple data sources, including those held locally with full security access controls.

aws

> “Chorus proved to be a valuable tool during the investigation and preparation for court.”
>
> - Major Crime Investigator

Demo and free trial

Try before you buy! take a 30-day trial of the Chorus Intelligence Suite

Our promise

To assess and realize the maximum benefits of the Chorus Intelligence Suite, we offer free 30-day trials for all our products, to be used on your own live cases.

Our entire organization is geared towards fully supporting you.

You will be assigned a Business Development Manager to scope your trial and to ensure your objectives are captured.

You will benefit from a dedicated Customer Success Manager to help you get the best out of the software. They will work with you to capture feedback, give you hints and tips, organize your implementation and schedule your training.

Our helpdesk will also be on hand to help you with any technical support.



Trial the CIS for free



A dedicated Customer Success Manager to support you every step of the way

Why Chorus?

About us

Chorus Intelligence is an award-winning international software company, providing law enforcement agencies with cutting-edge software.

The Chorus Intelligence Suite (CIS) supports agencies in reengineering their digital investigations, providing them with the tools to confidently collect, combine and connect data and turn it into intelligence and evidence.

Founded in 2011, Chorus is implemented throughout North America and is also used by 80% of UK police forces, all counter-terrorism units, and many government agencies.

Customer-focused

Over 90% of the functionality within the CIS can be directly linked back to a customer request.

We have an experienced professional services team for any customization or configuration of reports and interfaces.

Tailored training

Chorus provides accredited training courses to help our customers get maximum value out of the CIS.

The courses have been designed and written by experienced law enforcement and intelligence analysts who are experts in Chorus' suite of products. Chorus can also deliver custom training.

Our experts

Our entire team are experts in their field.

We combine former law enforcement Chiefs, Analysts, Investigators and open-source experts with software developers that specialize in police and financial data.

What our customers say

Trusted by North American law enforcement, over 80% of UK police forces and government agencies

"We set out to re-engineer our analytical capabilities and sought a solution that would support us in maximizing our operational effectiveness and time efficiency, while providing the best possible return on investment. The CIS will enable us to achieve this and set a precedent for intelligence-led, data-driven policing going forward."

- Chief Paul Neudigate, Virginia Beach Police Department

"The time spent analyzing data has been cut to a fraction of that used prior to having Chorus available."

- Investigator

"Chorus is by far the most significant aid to intelligence technology this century"

- Investigator

Without Chorus, the work I undertook would have been much more difficult and protracted, adding considerable time delays to the investigation and stress to the victims

- Lead Analyst

Discover · Link · Solve

CAD / RMS

3rd Party Data

Social Media

Internal Data

Phone Data

Hashtags #

Consented Data

Financial Data

Chorus

Empowerment Through Data



Discover · Link · Solve

Contact us.

Chorus Intelligence Inc

4525 Main Street, Suite 710

Virginia Beach

VA 23462

Request a demo or free trial

NASales@chorusintel.com

+1 888-688-6842

chorusintel.com



Chorus

Empowerment Through Data

CJIS SUPPORT SERVICES
CRIMINAL JUSTICE INFORMATION SYSTEM **617.660.4710**
FAX: 617.884.4601

THE CJIS REPRESENTATIVE'S GUIDEBOOK

Revised:

TABLE OF CONTENTS

CJIS REPRESENTATIVE RESPOSIBILITIES……1

CJIS GUIDELINES AND PROCEDURES……2

Compliance policies……..…2
Administrative Responsibilities of the CJIS Representative……..…2
Regional Working Groups……5
System Discipline……..6
Personnel Security……7
DCJIS User Agreement……8
Secondary Dissemination……9
III/CORI Information Disposal……9
Second Party Check……9
Hit Confirmation……9
CJIS Misuse……10
Retention of Hard Copy Printouts……10
CJIS/NCIC Error Messages……..10
Packing the Record……11
Memorandums of Understanding……11
Annual NCIC Purge……11
Record Retention Period……11
Offline Searches……..13
Security Incident Reporting……13
Felony Fingerprinting……..14

COMPLIANCE AUDIT……15

Questionnaire……..16
Policy Procedure Review……..16
Data Quality Review……..17
Accuracy……17
Completeness……17
Timeliness……17
Security……17
Dissemination……..…17
Documentation……17
Response Timeframe……17
Compliance Audit Review……18

VALIDATIONS……18

Validation Definition……19
Validation Responsibility……19
Validation Schedule……19
Validation Notification……19
Obtaining Validation Record Summary……21
Source Documentation……...22
Validation of Each record……22

SECURITY AWAREMESS TRAINING……28

Level One Certification……28
Level Four Certification……28
Local Agency Security Officer (LASO) Certification……..…30

SYSTEM AUDITING AND ACCOUNTABILITY…….……30

Auditable Event and Content……30
Events……31
Content……..…31
Response to Audit Processing Failure……32
Audit Monitoring, Analysis, and Reporting……..……32
Time Stamps……32
Protection of Audit Information……..32
Audit Record Retention……..32

APPENDIX A - TERMS AND DEFINITIONS

APPENDIX B - CJIS ONLINE

APPENDIX C - FORMS AND AGREEMENTS

CJIS REP Responsibilities

The CJIS Representative is an agency representative designated by the administrative head of a criminal justice agency. The administrative head, or Agency Administrator, is an individual within a criminal justice agency who has authority over the ORI and may designate duties as well as exercise authority for the agency. The CJIS Rep is responsible for their agency's use of the Criminal Justice Information System (CJIS) data. When a new CJIS Rep is appointed at an agency, DCJIS must be notified by the agency administrator by mail, email, or fax. If an Alternate CJIS Rep is going to be assigned, the CJIS Rep or administrator must notify DCJIS by mail, email, or fax. The CJIS Rep is responsible for making sure all Users, Non-access Users, and Non-Users within their agency have fingerprint supported background checks completed.

DCJIS is responsible for assisting agencies with access to CJIS systems. DCJIS provides the NCIC Operating Manual, NCIC Code Manual, and Nlets Manual for these reasons. DCJIS also offers classroom instruction for training purposes.

The employing criminal justice agency agrees to abide by all present laws, administrative rules, policies, and procedures of CJIS data as adopted by the Massachusetts Legislature and approved by the Commissioner of Public Safety and State Attorney General.

Summary of CJIS REP Responsibilities

- Dissemination, privacy, security of all DCJIS files – Security Incident Reporting
- Criminal Justice Agency Agreement
- Agency ORI validation – TQ/QO
- Fingerprint Submissions for all Users/Non-users – Pre-Employment Screening
- Notifying DCJIS to create and delete accounts
- User and non-user Security Agreements – Non-Disclosure Agreements
- Training and testing all users – Nextest – CJIS Online - LASO
- Audits
- Policies and Procedures – Misuse of CJIS reporting
- Validations
- Attending Regional Working Group Conference
- Record Entry - Timeliness – Accuracy – Hit Confirmation

GUIDELINES AND PROCEDURES

Purpose: To assist the CJIS Representatives in meeting CJIS compliance policies as set forth in the CJIS User Agreement.

Contents: CJIS Major Compliance Policies
General Information
Training/Certification Program
Validation Program

COMPLIANCE POLICIES – ADMINISTRATIVE RESPONSIBILITIES OF THE CJIS REP

For your reference listed below are some of the major CJIS Compliance policies set-forth in the User Agreement. For a more complete list refer to the User Agreement on the DCJIS Extranet.

1. A CJIS Representative and Backup CJIS Representative shall be appointed by the head of each Terminal Agency. The agency head will allow the CJIS Representative sufficient time to perform all necessary duties related to CJIS Responsibilities. The CJIS Representative and his or her agency will be responsible for monitoring terminal use, enforcing system discipline, and assuring that CJIS Operating Procedures are followed by all terminal USERs, as well as other related duties outlined in the CJIS User Agreement. In the absence of the CJIS Representative, the Backup CJIS Representative will be responsible for performing the duties of the CJIS Representative.

2. "803 code of Massachusetts Regulations 7.05 states, in part, that the department head of each agency shall submit a new user agreement to the CJIS Support Services (CSS) Unit bi-annually, or within 10 days upon the designation of a new CJIS Representative, back-up Representative, or appointment of a new agency head."

3. "Each CJIS terminal must be under the management control of a Criminal Justice Agency. Management control is defined as the authority to set and enforce: (1) priorities; (2) standards for the selection, supervision, and termination of personnel; and (3) policy governing the operation of the CJIS terminal."

4. "The data stored in the CJIS is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. Information obtained either from or through CJIS can only be used by law enforcement and criminal justice personnel in the performance of their authorized criminal justice activities. It is therefore incumbent upon an agency operating a CJIS terminal to implement the necessary procedures to make that terminal secure from any unauthorized use. Any departure from this responsibility warrants the removal of the offending agency from further CJIS participation."

5. "Section 7.06 of 803 CMR, and CJIS, and FBI/NCIC policy, require each TA to conduct a criminal record check on all agency personnel who have access to the CJIS terminal. This process must include a fingerprint-supported check of the Massachusetts State Bureau of Identification and FBI Identification Files."

6. The CJIS Representative is responsible for ensuring that all CJIS terminal and mobile data

terminal (MDT/MDC) operators in his/her agency are trained, tested, and certified as terminal operators within six (6) months of employment. Additionally, the CJIS Representative is responsible for ensuring that all individuals with access to secure areas where CJIS terminals are located, and/or where CJI is processed are trained and certified. Additionally, the CJIS Representative is responsible to ensure all agency vendors with access to the network where CJIS is located are fingerprint supported background checked and have completed the CJIS Online training certification. The Local Agency Security Officer (LASO) must complete the training certification at CJIS Online.

7. "A log of all secondary dissemination of III data must be maintained. Secondary dissemination is defined as the dissemination of any III response to another Criminal Justice Agency or an individual within another criminal justice agency or to anyone legally entitled to receive such information who is outside the original receiving agency. Each log entry must be maintained for at least twelve (12) months."

8. "Each TA must ensure that documentation is available to assist in the state and national audit programs"

9. "Every TA which enters records into CJIS and NCIC must ensure that hit confirmation is available for those records 24 hours a day".

10. "Any terminal agency, which provides CJIS, services to one or more non-terminal agencies must execute a memorandum of understanding (MOU) with each non-terminal agency to which it provides services. The MOU must detail the scope of services to be provided and must specify each agency's responsibilities as they pertain to any records entered into CJIS, or services provided on behalf of the non-terminal agency. Each agency must forward a copy of each executed MOU to the CJIS Support Services Unit (CSS) within 14 days of execution. A new MOU must be executed each time a new agency head has been appointed. A standard MOU may be obtained from the DCJIS Extranet."

11. "Any server agency which provides CJIS services to one or more MDT/MDC via a regional network, the server agency (HOST) must execute a mobile data terminal (MDT) agreement with each user agency (user) to which it provides services. The (MDT) agreement must detail the scope of services to be provided and must specify each agency's responsibilities as they pertain to any records entered into CJIS, or services provided on behalf of the user agency. Each agency must forward a copy of each executed (MDT) agreement to the DCJIS's CJIS Support Services Unit (CSS) within 14 days of execution. A standard (MDT) agreement may be obtained from the DCJIS Extranet."

12. "Any agency which receives a record in response to a CJIS and NCIC inquiry must confirm the record prior to arresting a wanted person, detaining a missing person, or seizing stolen property."

13. "After confirming a record, the agency taking a person into custody or seizing property must place a locate on the corresponding CJIS and/or NCIC record. If an agency receives multiple CJIS only records in response to an inquiry, it must place a locate on each active record in CJIS."

14. "When an agency receives a telephone request for a status confirmation on one of its records, it must respond to that request immediately by either confirming or rejecting the validity of the record or providing an approximation of the period of time that will be required to confirm the record's validity."

15. "When an inquiry on an individual or a piece of property yields a valid positive response (hit), the

printout showing the record(s) on file should be retained for use in documenting probable cause for the detention of the missing person, arrest of the wanted person, or seizure of the property. The printout may also prove valuable in a civil suit alleging a false arrest, a false imprisonment, a civil rights violation, or an illegal seizure of property."

16. "When an inquiry yields a hit, the terminal operator making the inquiry should note on the printout the name of the person confirming the record (if confirmed by telephone), as well as the date and time that the record(s) was confirmed. In addition, the operator should note precisely how, when, and to whom the information was given, initial and date this notation, and forward the printout to the inquiring officer or agency for retention in the case file. This procedure establishes the chain of evidence for the communication should the arresting officer need to substantiate his or her actions in a judicial proceeding."

17. "Any TA having record entry capabilities must enter records into CJIS and NCIC which meet established criteria as soon as possible."

18. "M.G.L. c.22A, S.4, states that,"[W]henever a parent, guardian, or governmental unit responsible for a child, reports to any police officer or law enforcement official that a child is missing, such police officer or official shall immediately cause to be entered into the central register relevant information relative to said missing child. Such police officer or law enforcement official shall also immediately undertake to locate such missing child..."

19. "A complete record of any kind includes all information that was available on the person or property at the time of entry. An agency must consult with investigators, review case files, and make inquiries of the CJIS and NCIC Wanted, Missing, and Stolen Property, WMS, BOP, Triple I (III), Automated Name Index (ANI), and appropriate registry of motor vehicles files. The validation process must include a review of whether additional information has become available since the original entry was made. Any additional information must be added to the record when it is possible to do so."

20. "A second party must verify the accuracy of a CJIS and NCIC record. This second party check should include assuring that the required crosschecks (e.g., VIN and license plate number, etc.) were made, and that the data in the CJIS and NCIC entries match the data in the investigative report. Agencies lacking support staff for this cross-checking should require the case officer to check the record as he/she carries the primary responsibility for seeking the fugitive and/or stolen property."

21. "Immediately upon a warrant being issued and, for NCIC entry purposes, an extradition determination has been made by the district attorney's office, or the warrant meets the NCIC requirements for the use of 'NOEX' as outlined in the CJIS Operating Manual. The Date of Warrant (DOW) field must contain the date that these events occurred."

22. "A timely modification of any record is one made upon receipt of additional or different information."

23. "A timely removal of any record from CJIS and NCIC is one made immediately upon notification that a Wanted/Missing Person has been apprehended or located, or that Stolen Property has been recovered. In addition, a record must be cancelled when it cannot be properly validated."

24. "M.G.L. c.40, Section 36A, states, in part, the following: "Whenever a person in police custody attempts or threatens suicide at a lockup facility, the officer in charge of the lockup shall, within twenty-four hours of such incident, record in the criminal history systems board computer the name,

address, and the age of such person, the charge or reason for such detention and the nature and date of said attempt or threat..."

25. "Any person who attempts, or threatens to attempt, to commit suicide, while in the custody of a law enforcement or criminal justice agency, MUST be entered into the Suicide Risk file by that agency WITHIN 24 HOURS OF THE INCIDENT."

26. "An entry into the Suicide Risk file MUST be made for EACH threat or attempt made by an individual while in custody."

27. Each agency having records in CJIS and NCIC is required to validate a portion of those records each month. Records to be validated are obtained using the on-line validation program."

28. "Any TA which enters records for a non-terminal agency must ensure that those records are validated by the non-terminal agency in accordance with the above guidelines. The TA shall cancel any record(s) which the non-terminal agency fails to validate within a specified time period determined by the TA.

29. "The entering agency has the primary responsibility for the entry and maintenance of accurate, timely, and complete records. Accordingly, each terminal agency must institute appropriate and reasonable quality assurance procedures. Each TA must also implement security and personnel training standards which ensure valid and accurate records and appropriate dissemination of same."

30. "Each agency is responsible for its own records and must always have personnel available to make required corrections and changes. Alterations must be made immediately, and not be left for personnel working subsequent shifts. Each agency must have stringent procedures which ensure that all records are kept accurate, complete, and up to date."

31. "The CJIS Representative shall ensure that any publications distributed by the DCJIS are, in turn, distributed to appropriate personnel in his/her agency. Consistent with this provision, the CJIS Representative shall coordinate distribution within his/her agency of the CJIS Operating Manual, the NCIC code manual, and as requested, other publications provided to enhance effective use of the CJIS and NCIC systems."

32. "Each CJIS Representative and/or back up Representative shall attend the biannual regional working group meetings. If the Representative or back up Representative is not available to attend, the Representative may designate another agency employee to attend."

REGIONAL WORKING GROUPS - RWG

DCJIS has created seven (7) Regional Working Groups within the Commonwealth. Each terminal agency within each region shall appoint one (1) Representative to serve as a general member of the Regional Working Group. In addition, each Regional Working Group shall elect three (3) Representatives to serve as Chairperson, First Vice-Chairperson and Second Vice-Chairperson of the region. The Chairs for each region shall comprise a body known as the Advisory Policy Board (APB).

The twenty-one (21) member Advisory Policy Board (APB) shall elect three (3) Representatives to serve as its Officers; Chairperson, First Vice-Chairperson and Second Vice-Chairperson.

Regional working groups are formulated to:

- Improve the effectiveness of the criminal justice system through the efficient automated exchange of documented criminal justice information.

- To foster and cement relationships among diverse criminal justice professionals.

- To exchange ideas and information on changing technology within the criminal justice community.

Regional Work Groups hold meetings annually. These meetings shall take place in the Spring or Fall of each year. In addition, informal meetings may be held at the discretion of the region.

Representatives for each terminal agency shall be required to attend the Spring or Fall RWG meetings. Attendance at other meetings which may take place during the year shall be voluntary.

Each CJIS Representative MUST attend the annual RWG meetings. If the CJIS Representative is unable to attend, the Representative may designate a proxy from his/her agency to attend the meetings in his/her absence.

SYSTEM DISCIPLINE

1. To help ensure the proper operation of the CJIS/NCIC Systems, the standards, procedures, formats, and criteria mentioned in the CJIS Manual and the CJIS Training Guides must be strictly followed. In this respect, CJIS must not only follow the rules set forth but must also ensure that agencies they are servicing do the same.

2. Complete, accurate, and timely records are essential to ensure System Integrity. Users also are encouraged to enter records in a timely manner to afford the maximum protection to the law enforcement officer by providing up-to-date information. Although the use of CJIS/NCIC is voluntary, delayed entry of records reduces or eliminates the possibility of apprehending wanted persons, locating missing persons, and recovering stolen property.

3. Promptness in modifying, locating, or canceling records in the System will help to keep the System free of outdated information.

4. CJIS/NCIC provides information for decision making by investigators, patrol, officers, judges, prosecutors, and corrections officials. The information furnished by CJIS/NCIC must be evaluated along with other facts known to the officers, investigators, judges, prosecutors, and corrections officials.

5. When an agency receives a positive response from CJIS/NCIC and an individual is being detained or a piece of property can be seized, an immediate confirmation with the agency that originated the record in the System is necessary. This confirmation ensures the validity of the hit before an arrest or seizure is made. Likewise, the originating agency has the duty to respond promptly with the necessary confirmation and other pertinent details. (Refer to Hit Confirmation)

PERSONNEL SECURITY

Record Checks on Agency Personnel

Section 7.06 of 803 CMR, and CJIS and FBI/NCIC policy, require each TA to conduct a criminal record check on all agency personnel who have access to the CJIS Terminal. This process must include a fingerprint-supported check of the State Identification Section (SIS) and FBI Identification Files. Additionally, anyone with unescorted access within a secure area where a CJIS terminal is located also require a fingerprint supported background check. (This includes custodial staff).

Thorough personnel background screening by the employing agency is required for terminal operators, programmers, and other persons employed or utilized to effectuate access to, or initiate transmission of, CJIS/NCIC information. Appropriate background investigations, including submission of completed applicant fingerprint cards to the FBI Identification Division and the State Identification Section (SIS), must be conducted on all new CJIS terminal operators before system access is granted.

1. The employing agency must check state and national arrest and fugitive files.

2. If a record of any kind is found, the agency to which the applicant has applied for employment and/or CJIS access will be formally notified indicating CJIS access will be delayed pending review of arrest and fugitive records.

3. When identification of the applicant has been established by fingerprint comparison and he/she appears to be a fugitive or to have an arrest history for a felony or misdemeanor, an agency head or his/her designee will review the matter. If the applicant is found to be a fugitive from justice, or to have been convicted of a felony or misdemeanor, the matter will be referred to DCJIS' Field Services Unit.

4. If a determination is made that CJIS access by the applicant would not be in the public interest, such access will be denied, and the applicant's appointing authority will be notified in writing of the access denial.

Departments and agencies may submit one applicant card per applicant (Form I-9 blue and white card) to the SIS for criminal justice employment checks. All applicant cards submitted to the SIS must include a 13-character alphanumeric tracking number in the designated space on the card (see below example). Applicant tracking numbers must be **unique to the fingerprint card submission and cannot be re-used**. A Second FBI Applicant (Blue) card must be submitted through the SIS, who will forward to the FBI. These Applicant Cards MUST contain the ORI of the agency that requires the response to the record check.

In most cases the ORI on the print card will be the agency submitting the print card to the SIS.

Criminal Justice Employment (example):

- A (applicant)
- BOS (3 characters CJIS Agency Code)
- 2000 (4 characters indicating the year)
- 00001 (5 characters - sequential numbering beginning with first submission of calendar year)

Departments mailing or hand-delivering ten print cards must address/deliver them to:

Massachusetts State Police
Identification Section
59 Horse Pond Road
Sudbury, Massachusetts 01776

These submissions will be processed as received, and responses will be returned to the submitting department via fax. If you need additional ten print cards (criminal and applicant), please call 508-358-3171.

In the event an agency wishes to allow access to an individual who fails the screening criteria, a written request to the CSO requesting access must be submitted.

The written request must contain the following information:

a. Subject's name.

b. Subject's date of birth.

c. Subject's social security number.

d. Length of employment with agency.

e. Job title.

f. Type of CJIS access.

g. Arrest and disposition information along with copies of any documentation obtained by the agency regarding the disposition.

h. The request must also state that the agency has disciplinary procedures in place for misuse of CJIS information and the agency will accept responsibility and liability for any misuse of CJIS information initiated by the subject.

USER AGREEMENT

803 Code of Massachusetts Regulations 7.05 states, in part, that DCJIS as the CJIS Systems Agency (CSA) "shall cause each user of CJIS to execute a User Agreement."

This User Agreement sets forth the mutual responsibilities of the DCJIS and each terminal agency on the CJIS network.

Each terminal agency must submit a new User Agreement bi-annually.

Exception, when an agency designates a new CJIS Representative, Backup Representative, or if a new Agency Head has been appointed, then a new CJIS User Agreement will be submitted to CJIS, within ten (10) days."

The User Agreement is available via the CJIS Extranet.

SECONDARY DISSEMINATION

Secondary dissemination is defined as any dissemination of III (or any CORI information) response to another criminal justice agency or an individual within another criminal justice agency. An agency MUST record secondary dissemination either in its CORI Dissemination Log or in a separate III Log. Each log entry MUST be retained for at least one year.

This log shall contain at a minimum: the date and time of inquiry, the name and date of birth of the subject inquired on, and the name of the individual who is requesting the III record. Additionally, the log should also contain the item disseminated, the reason for dissemination, and the method of dissemination.

III/CORI INFORMATION DISPOSAL

When the retention of III records (or any CORI information) is no longer required, each agency must dispose of responses in a secure manner to preclude unauthorized access/use, this may be accomplished by shredding the information, etc.

III and CORI is sensitive and should be treated accordingly, an unauthorized request or receipt of such material could result in criminal proceedings.

SECOND PARTY CHECK

Every TA (terminal agency) which enters records into the CJIS and NCIC systems must have a policy in place to ensure a second party check.

A second party must verify the accuracy of a CJIS and NCIC record. This second party check should include assuring that the required cross-checks (e.g., VIN and license plate number, etc.) were made, and that the data in the CJIS and NCIC entries match the data in the investigative report. Agencies lacking support staff for this cross-checking should require the case officer to check the record as he/she carries the primary responsibility for seeking the fugitive and/or stolen property.

HIT CONFIRMATION

When an agency receives a request for a status confirmation on one of its records, it must respond to that request immediately by either confirming or rejecting the validity of the record or providing an approximation of the period that will be required to confirm the record's validity.

Every TA (terminal agency) which enters records into CJIS/NCIC must assure that hit confirmation is available for all records, except III records, 24 hours a day either at that agency or through a written agreement with another agency at its location.

CJIS MISUSE

Criminal Justice Information (CJI) is the term used to refer to all CJIS provided data necessary for law enforcement to perform their mission including, but not limited to biometric, identity history, biographic, property, and case/incident history data. Access to CJI is for official law enforcement purposes only. CJI must be used for the purpose for which it was provided and afforded the maximum protection. It is forbidden for agency personnel to request and/or perform inquiries for curiosity, including running your own personal information. Any inquiry other than a criminal justice purpose must be governed by a federal, state, or local statute(s).

There are several statutes and regulations may apply in the case of improper access to, or dissemination of CJIS. If the information involved access to CORI, there are both civil and criminal penalties. The civil penalties include up to a $5,000 fine issued by the DCJIS Criminal Record Review Board pursuant to MGL c. 6, s. 168. The criminal penalty for a CORI violation is set forth in MGL c. 6, s. 178 and includes up to one year and/or a $5,000 fine.

DCJIS regulation violations include a violation of 803 CMR 7.09 pertaining to improper access and use of CJIS data.

If the information involved access to FBI CHRI records, then it would also be a violation of federal regulation 28 CFR 20.33. Additionally, improper access and dissemination of RMV records is also a violation of 18 USC. 2721.

Lastly, there are also criminal penalties for improper use of a computer, see MGL c. 266, s. 120F."

RETENTION OF HARD COPY PRINTOUTS

When an agency receives a locate message on one of its records, or an inquiry on an individual or a piece of property yields a valid positive response (hit), the printout showing the record(s) on file should be retained for use in documenting probable cause for the detention of the missing person, arrest of the wanted person, or seizure of the property. The printout may also prove valuable in a civil suit alleging a false arrest, a false imprisonment, a civil rights violation, or an illegal seizure of property.

All hard copy printouts of record entry, modification to record, and/or a record cancellation message must be retained in the agency's case files.

The printouts should be retained for as long as there remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. Retain the printout until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated.

CJIS/NCIC ERROR MESSAGES

Each agency is responsible for its own records and must always have personnel available to make required corrections and changes. Alterations must be made immediately, and not be left for personnel working subsequent shifts. Each agency must have stringent procedures which ensure that all records are kept accurate, complete, and up to date.

CJIS and NCIC monitor records for errors and when an error is detected, the entering agency will receive an Administrative Message from the CSS or Unsolicited Message from NCIC regarding the record in question. Where possible, the staff will assist in obtaining the correct information. The message will state that if the record is not cancelled or corrected within 24 hours, it will be removed from the CJIS and NCIC computer systems.

Twenty-four hours after the message is sent, the CSS will make an inquiry on the record in question. If the record has not been cancelled or corrected, the CSS will cancel the record.

Each agency is responsible for its own records and MUST always have personnel available to make required cancellations or corrections with the assistance of the CSS staff. Additionally, each agency must implement stringent procedures to ensure that all records are kept accurate, complete, and up to date.

PACKING THE RECORD

A complete record of any kind includes all information that was available on the person or property at the time of entry. An agency must consult with investigators, review case files, and make inquiries of the CJIS and NCIC Wanted, Missing, and Stolen Property, WMS, BOP, Triple I (III), Automated Name Index (ANI), and appropriate registry of motor vehicles files. Any additional information obtained after the time of entry must be added to the record.

MEMORANDUM OF UNDERSTANDING

Any terminal agency which provides CJIS services to one or more non-terminal agencies must execute a memorandum of understanding (MOU) with each non-terminal agency to which it provides services. The MOU must detail the scope of services to be provided and must specify each agency's responsibilities as they pertain to any records entered into CJIS, or services provided on behalf of the non-terminal agency. Each agency must forward a copy of each executed MOU to the DCJIS's CJIS Support Services Unit (CSS) within 14 days of execution. A new MOU must be executed each time a new agency head has been appointed. A standard MOU may be obtained from the CJIS CSS by calling 617-660-4710.

THE ANNUAL PURGE

Each January, the data center conducts the Annual Purge of the CJIS data files. This purge removes from the database all records which have passed their respective retention periods.

Any record which is removed as the result of the annual purge may be re-entered by the originating agency. The only exceptions to this option are License Plates and Boat Registrations which have expired, these MAY NOT be re-entered.

RECORD RETENTION PERIOD

Unless otherwise removed or located, records will be retained in file as follows:

Article File	-	Balance of the year entered plus one (1) year.
ATF Violent Felon File	-	Indefinitely or until ATF removes record.

Boat File	-	Balance of the year entered plus four (4) years.
Deported Felon File	-	Indefinitely or until removed by Immigration and Naturalization Service.
Foreign Fugitive File	-	Indefinitely or until removed by the ORI.
Gun File	-	Indefinitely or until removed by the ORI. Recovered weapons will remain for the balance of the year entered plus two (2) years.
III Records	-	Until the individual reaches the age of 99.
License Plate File	-	Records remain for one (1) year after the end of the plate's expiration year. Records for non-expiring license plates remain for the year of entry plus four (4) years.
Missing Person File	-	Indefinitely or until removed by the ORI.
ORI File	-	Indefinitely. If an agency no longer qualities for NCIC access, the ORI record is retired, but kept in an inactive status.
Parts File	-	Balance of the year entered plus four (4) years.
Securities File	-	Balance of the year entered plus four (4) years, except records for traveler's checks and money orders which are retained for the balance of the year entered plus two (2) years.
Suicide Risk File	-	Indefinitely.
Unidentified Person File	-	Indefinitely or until removed by the ORI.
US Secret Service Protection File	-	Until removed by the Secret Service.
Vehicle File	-	Balance of the year entered plus four (4) years. Felony Vehicle records and records not containing a VIN or OAN will remain for ninety (90) days after entry. License data in a vehicle record are purged one (1) year after the plate's expiration year.
Violent Gang and Terrorist Organization File	-	GMC records - are retained five (5) years unless removed by originating agency. Only records entered by Corrections agencies remain past five years. GRC records - Single Interest - indefinitely or until removed by originating agency. Multiple Interests - indefinitely or until **all** agencies remove their records.
Wanted Person File	-	Indefinitely or until removed by the ORI.

Temporary felony wanted records will be automatically removed after 48 hours.

OFF-LINE SEARCHES

An off-line search is a special technique to obtain from the CJIS and/or the NCIC database, information which cannot be obtained through your agency terminal. Off-line searches are performed for a variety of circumstances.

Off-line searches can be performed with a minimum amount of information (e.g., certain time frame, partial plate number, personal descriptors, partial VIN, etc.); however, searches including all available information may be more efficient and effective.

Searches may be run against two sources of data:

- Active Data; or
- Historical Data

To obtain an off-line search you must:

1. Complete the Off-Line Search Request form which is located on the DCJIS Extranet, or in exigent circumstances use agency stationary and explain the type of search you are requesting, including all available information to help narrow the search.
2. It must be signed by the Agency Head or designee.
3. Email the request to cjisoffline@mass.gov.
4. The report will be emailed secure to your agency.

Note: If you have a preference as to how you want to receive the results, it must be added to the letter of request.

SECURITY INCIDENT REPORTING

Massachusetts criminal justice agencies are reminded that any security incidents involving access, or potential access, to department systems or networks, or to criminal justice information of any kind, ***must*** be reported within forty-eight (48) hours to the Department of Criminal Justice Information Services (DCJIS), regardless of whether the incident involved the CJIS network or CJIS systems. This requirement is contained within the CJIS User Agreement, which is signed by the department Agency Head, CJIS Representatives, and CJIS Technical Contact. Specifically:

Incident Reporting – A security incident is violation or a potential violation of the

> confidentiality, integrity and/or the availability of state/FBI CJIS data. If such an incident should occur, the agency head shall submit a fax, on agency letterhead…to (617) 884-4601 within forty-eight hours with the following information:
>
> - Date & Location of incident
> - Systems affected
> - Method of detection & Nature of Incident
> - Description of the incident & Actions taken/resolution
> - Date & Contact information for the agency

Further, the FBI's CJIS Security Policy also has ***mandatory*** policy and reporting requirements for computer security breaches:

> Incident Response – …Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, (ii) track, document, and report incidents to appropriate agency officials and/or authorities.
>
> Reporting Information Security Events – The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

In lieu of the fax on agency letterhead described in the CJIS User Agreement, the DCJIS has created a Computer Incident/Security Form which must be used to notify the DCJIS of such events. The form is posted online on the DCJIS Extranet.

Please direct any questions about this procedure to the CJIS Support Services Unit at 617.660.4710 or via email at cjis.support@mass.gov.

FELONY FINGERPRINTING

Pursuant to M.G.L. c. 263, § 1A and 803 CMR 7.08, the Department of Criminal Justice Information Services ("DCJIS") is tasked with auditing law enforcement agencies to ensure compliance with the statutory requirement that any person arrested and charged with a felony be fingerprinted. Fingerprinting should be completed by the arresting agency or by another law enforcement agency on behalf of the arresting agency using the Originating Agency Identifier ("ORI") of the arresting agency.

Specifically, M.G.L. c. 263, § 1A states as follows:

> Whoever is arrested by virtue of process or is taken into custody by an officer and is charged with the commission of a felony shall be fingerprinted according to the system of the department of state police and photographed. The fingerprints and photographs shall

> be immediately forwarded to the department of state police to allow a biometric positive identification. The fingerprint record shall be suitable for comparison and shall include an offense-based tracking number, completed description of the offenses charged and other descriptors as required. The executive office of public safety and security may audit police departments for compliance with this section.

Following from this, 803 CMR 7.08(1)(b) requires that "[f]ingerprints shall be submitted to the Massachusetts State Police State Identification Section" for "any felony arrest by a law enforcement agency, as required by M.G.L. c. 263, § 1A." Further, 803 CMR 7.08(5) provides that:

> DCJIS may audit any [criminal justice agency ("CJA")]'s fingerprinting practices and procedures to ensure compliance with M.G.L. c. 263, § 1A, and 803 CMR 7.00. In connection with any such audit, a CJA is required to respond to audit questionnaires, complaints, and/or any other inquiries from DCJIS within the time specified by DCJIS.

When DCJIS conducts the Felony Fingerprint audit an Excel spreadsheet containing a list of felony arraignments for the arresting agency will be provided. The last column header of the spreadsheet is the "Offense-Based Tracking Number (OBTN)." All fingerprint submissions must include an offense-based tracking number tied to a specific arrest event.

On the spreadsheet please provide the OBTN for the arrest that led to each arraignment, or in the event the individual was not fingerprinted, provide the reason why in the same OBTN column.

Each felony arraignment will ultimately fall into one of the following four categories:

> **No Fingerprint Record Located** – No record found for the person being arraigned.
> **Complaint/Summons** – Individual not arrested, appeared in court via summons or complaint.
> **Fingerprinted** – Felony arrest fingerprinted by the arresting department.
> **Fingerprinted by another agency** – Felony arrest fingerprinted by another agency on behalf of the arresting agency.

Once the audit is completed DCJIS will send a data quality review letter to you, and a copy of the review will be retained in our files.

COMPLIANCE AUDIT

The Department of Criminal Justice Information Services (DCJIS) is mandated to audit law enforcement agencies that access the DCJIS network at a minimum of once every three years. The audit is designed as a process for improving the criminal justice information system, not for imposing penalties. The objective of this audit is to verify adherence to CJIS and NCIC policies and regulations and is called a Compliance Audit. Audits may be conducted on a more frequent basis should it be necessary. The audit cycle begins on July 1st of the scheduled audit cycle and ends June 30th 3 years later. The CJIS Representative, back-up Representative, and security officer are required to be involved in the compliance audit of their agency.

The compliance audit consists of four sections: 1- Comprehensive CJIS questionnaire, 2- Policy and Procedure review, 3- Data Quality Review (for NCIC entering terminal agencies), 4- Physical Security Walk through. Once the compliance audit is completed the DCJIS auditor will conduct a review of the

audit and note any findings that may have been identified during the audit process.

DCJIS Policies and Procedure forms are located on the DCJIS Extranet under the Audit Tab.

There may be times due to an agency's audit results, or per an agency's request that an agency on-site audit will be conducted at the CJIS agency by one or more Field Representatives from the CJIS Field Services Unit. The Auditor(s) will interview appropriate agency personnel, asking questions relative to the agency's policies and procedures in effect at the agency as they relate to the usage of the CJIS and the NCIC computer systems.

QUESTIONAIRRE:

To begin the audit process, the agency being audited should have received an initial email from the DCJIS auditor who will be conducting the on-site audit. This pre-audit questionnaire is the second step in completing the audit; therefore, it is essential to return the completed questionnaire no later than the date noted in the e-mail. The pre-audit questionnaire does several things to help the audit process. First, it provides the agency with a description of what to expect during the on-site audit, including a general idea of the topic areas that will be discussed. Second, it requests a list of documentation and questions to be completed by the agency to assist the auditor in preparing for the actual on-site review process. Finally, the information obtained from this questionnaire affords the auditor with a fundamental insight into the agency's policies and procedures as they relate to policy requirements. Consequently, the scope of the audit can be narrowed to address questions related to the agency during the on-site audit. In addition, it is used to inform and prepare the auditor of the policies/procedures and/or requirements as they relate to each of the local agencies selected for the audit.

POLICIES AND PROCEDURES REVIEW:

This section of the compliance audit will address required local agency CJIS polices and Memorandums of Understanding (MOUs). Refer to appendix C for a list of policies and MOUs that are required if applicable to your agency.

The next section covered will be Terminal Operator training and certification (Nextest). Additionally, training and certification (CJIS Online) will be reviewed for those individuals without direct access to CJIS, however, will have access to secure areas where CJIS terminals are located and/or Criminal Justice Information (CJI) is processed.

A walk through of the areas where CJIS terminals are located and where CJI is processed will be conducted. This is to ensure proper security measures have been taken to limit the access to only individuals required to be in those areas and terminals are located so that screens are not facing public areas. Also, to ensure CJI is properly secured, and access is limited to only those individuals required to be in that area.

DATA QUALITY REVIEW:

This part of the audit consists of reviewing a sample of the agencies NCIC entries for accuracy, timeliness, and completeness. Entries for Wanted Persons, Missing Persons, and Stolen Vehicle will be reviewed. A maximum of 25 records in each section will be reviewed. The NCIC record entered by the agency will be compared to the physical case file records to determine if the entry is accurate, entered in a timely fashion, and contains any additional information that is noted in the case file above and beyond the minimum required entry information (Packing the Record).

ACCURACY

Each CJIS and NCIC record must be error free. In addition, the TA must maintain necessary documentation as required by CJIS and NCIC policy. Documentation must also be available from non-terminal agencies accessing CJIS and NCIC through the TA.

COMPLETENESS

The information in each CJIS and NCIC record constitutes all pertinent and available information.

TIMELINESS

The entry, update, and removal of records must be completed as soon as information supporting an entry, update, or removal becomes available.

SECURITY

The TA must protect its information against unauthorized access, ensuring confidentiality of the information in accordance with State and Federal law and with CJIS and NCIC policy.

DISSEMINATION

DOCUMENTATION

Each TA must ensure that documentation is available to assist in the audit program.

When an agency receives a printout of records to be reviewed as part of the audit, they must compare the records against their agency's documentation (e.g., case files) and/or other information available at the agency. Instructions are included with the record printouts and must be followed exactly. An agency will receive a random sample of ten percent (10%) of their records in a particular file. Agencies, which have many records in a particular file, will receive no more than 25 records in that file. Agencies, which have a small number of records in a particular file, may receive them all.

RESPONSE TIMEFRAME

Agencies have a 20-day response timeframe in which to return to the CJIS Support Services Unit the completed Audit Questionnaire, including all required documentation as listed below:

1.) the completed questionnaire

2.) a newly signed User Agreement

3.) a copy of the TQ and QO with corrected information (if applicable) for NCIC and NLETS

4.) the list of certified personnel – Nextest certification reviewed and updated

5.) a copy of the current maintenance contract

6.) a copy of the agency's internal procedures relating to the CJIS terminal

7.) a copy of the record printouts with all notations as directed in the record review instructions

8.) Up to date Memorandums of Understanding and required agreements are prepared

9.) All CJIS Users and non-users with unescorted access have had a fingerprint supported background investigation completed upon hire and every five years thereafter

10.) Review of agency vendors for completed fingerprint supported backgrounds and vendor agency and vendor employee agreements of non-disclosure and FBI Security Addendum

Upon receipt of the required documentation and on site audit the CJIS Support Services auditor will prepare a written report of the audit results. The original report will be forwarded to the agency and a copy of the report will be maintained at the CJIS Support Services.

If an agency is found to be out-of-compliance in one or more areas of the audit it will be noted, and a response from the TA (terminal agency) will be required within 30 days as to what action was taken to ensure compliance.

COMPLIANCE AUDIT REVIEW WITH AGENCY:

Once the on-site audit is completed the auditor will review with the CJIS Representatives those areas of the audit that met NCIC audit requirements. The auditor will also discuss issues with non-compliant areas of the audit and what will be needed to make the appropriate corrections. Additionally, the auditor will provide suggestions for those areas of the audit which would improve operational requirements.

The auditor will provide a written report of the overall compliance audit to the agency head and CJIS Representatives noting those areas where non-compliant issues will need to be addressed and reported in writing by the agency to DCJIS.

THE VALIDATION PROGRAM

Record validation is one of the most important components of any data quality program. Since the users of CJIS and NCIC are the primary source of the information contained within these systems, each agency with records in the CJIS and NCIC databases is a vital contributor to the data quality process and is directly responsible for the accuracy of its records. Therefore, to assist agencies with this important and serious responsibility, the CJIS and NCIC validation programs were implemented.

CJIS and NCIC policy require that each agency with records in these systems have specific, step-by-step procedures for validating those records. To help users comply with these policies, the CJIS Support Services Unit has developed the following model validation procedures. Each agency is encouraged to

implement these model procedures. At the very least, each agency must develop its own set of procedures, which are as comprehensive as those contained in the model. The CJIS Support Services Unit is available to assist each agency in the creation of validation procedures, which are tailored to the needs of the specific agency.

VALIDATION DEFINITION

Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must decide based on the best information and knowledge available whether to retain the original entry in the file. Validation procedures must be formalized, and copies of these procedures must be on file for review during an NCIC/CJIS audit.

VALIDATION RESPONSIBILITY

The integrity and validity of each record is clearly the responsibility of the agency that entered the record. Validation is one of many tools that assist the entering agency in maintaining the integrity of their records.

VALIDATION SCHEDULE

Each agency that enters records into the CJIS and NCIC systems is required to perform a monthly validation. The records to be validated each month are those which are 60-90 days old, 14-15 months old, 26-27 months old, 38-39 months old, etc. In other words, in April, an agency is required to validate all its records that were entered during the month of January of the current year and all previous years. The Validation Schedule is as follows:

VALIDATION MONTH:	RECORDS ENTERED MONTH:
JANUARY	OCTOBER
FEBRUARY	NOVEMBER
MARCH	DECEMBER
APRIL	JANUARY
MAY	FEBRUARY
JUNE	MARCH
JULY	APRIL
AUGUST	MAY
SEPTEMBER	JUNE
OCTOBER	JULY
NOVEMBER	AUGUST
DECEMBER	SEPTEMBER

VALIDATION NOTIFICATION

At the beginning of each validation cycle, the validation application within Messenger will generate an administrative message notification transaction to each ORI with records to validate providing a summary of the type and number of the records to be validated. In addition, DCJIS staff will send an e-mail message to the CJIS Representative and Back-up CJIS Representative notifying them that the current

validation is available for completion.

An example of the Messenger Notification message follows:

THIS MESSAGE SUMMARIZES THE JANUARY RECORDS REQUIRING VALIDATION BY ORI WITHIN 20 DAYS OF THIS NOTICE.

WANTED PERSON: 10
STOLEN VEHICLE: 20
PROTECTION ORDER: 5

TOTAL RECORDS: 35

FOR ADDITIONAL INFORMATION, THE VALIDATION QUICK REFERENCE GUIDE CAN BE FOUND ON THE CJIS EXTRANET. IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT THE CJIS SUPPORT SERVICES UNIT AT 617-660-4710.

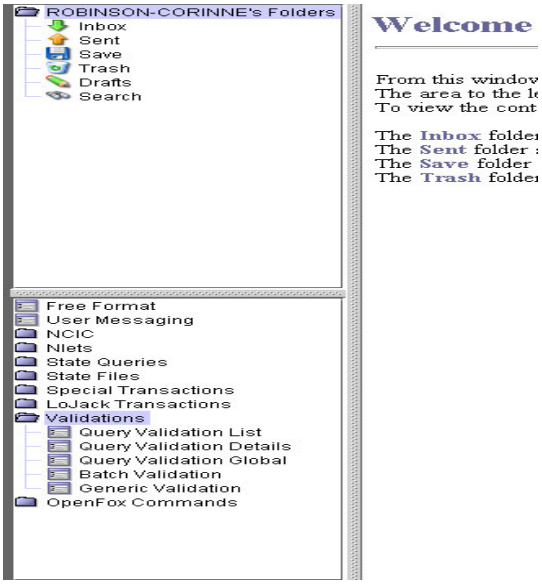
OBTAINING THE VALIDATION RECORD SUMMARY

To obtain the details of the records to be validated, the user must first conduct a Query Validation List (QVAL) transaction.

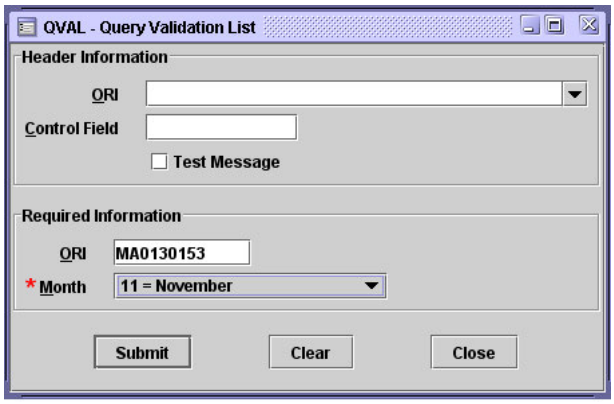
1. Type QVAL in the quick query bar located at the bottom of the CJIS Messenger Desktop and hit the enter key. (SkiptoStep3)

Or

In the Messenger forms tree, double-click on the Validations folder.



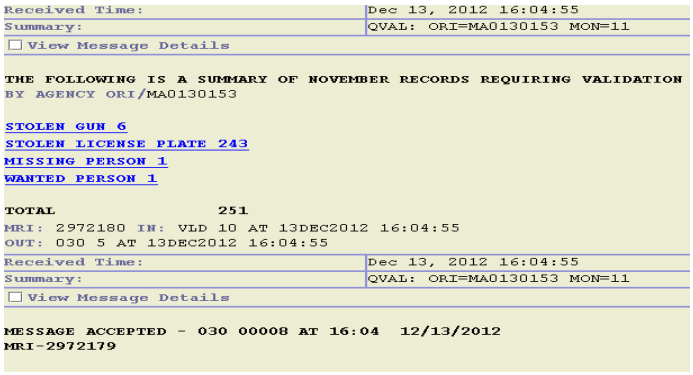
2. Double-click the "**Query Validation List**" link. The QVAL-Query Validation List form will be displayed.



3. Enter the ORI of your agency and then select the current month in the Month drop-down list.

Important: To validate the correct records, you MUST select the current month in the Month drop=down list.

4. Click the Submit button. A summary of the records requiring validation will be returned to your inbox.



OBTAINING DETAILED REPORT OF RECORDS TO BE VALIDATED

To obtain the actual detail of each record requiring validation, click the link for each file type shown in the QVAL response.

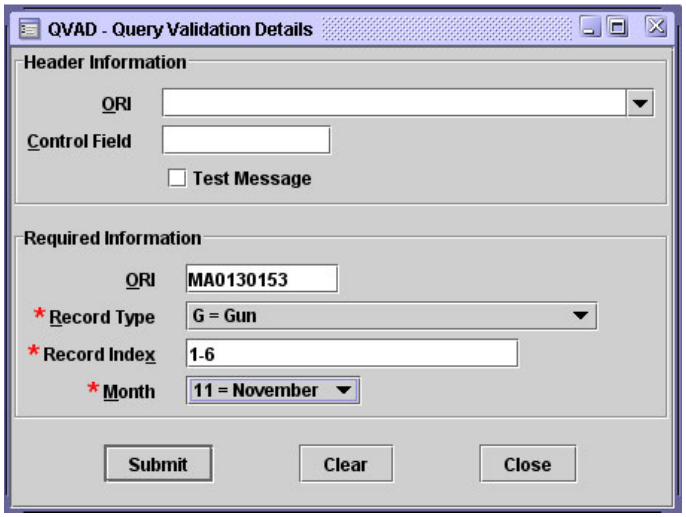
Alternatively, you may complete a Query Validation Detail (QVAD) transaction as follows:

1. Type QVAD in the quick query bar located at the bottom of the CJIS Messenger Desktop and hit the enter key. (Skip to Step 3)

   Or

   In the Messenger forms tree, double-click on the Validations folder.

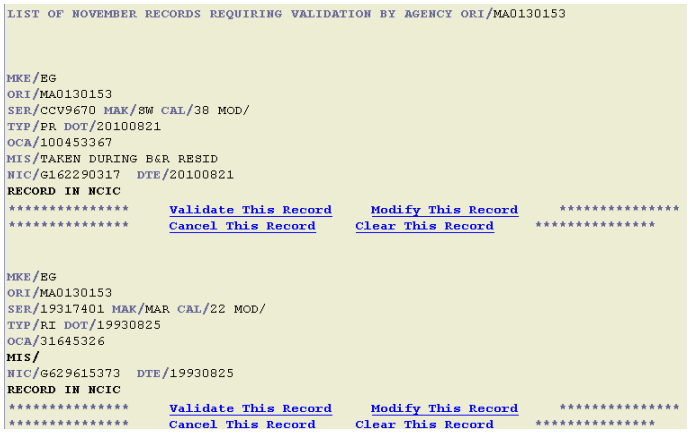
2. Double-click the "**Query Validation Details**" link. The QVAD-Query Validations Details form will be displayed.



3. Enter the ORI of your agency, select the record type of the file you are validating, enter the record index (records 1-X of the records to be validated in the selected file), and select the current month in the Month drop-down list.

4. Click the Submit button. A detailed listing of each record to be validated in the selected file will be returned to your inbox.

Note: only the records entered in the record index will be returned. In the example above, records 1-6 in the gun file would be returned. You may have to conduct multiple QVAD transactions to see all of the records you need to validate in a given file.


LIST OF NOVEMBER RECORDS REQUIRING VALIDATION BY AGENCY ORI/MA0130153

MKE/EG
ORI/MA0130153
SER/CCV9670 MAK/SW CAL/38 MOD/
TYP/PR DOT/20100821
OCA/100453367
MIS/TAKEN DURING B&R RESID
NIC/G162290317 DTE/20100821
RECORD IN NCIC
********** Validate This Record Modify This Record **********
********** Cancel This Record Clear This Record **********

MKE/EG
ORI/MA0130153
SER/19317401 MAK/MAR CAL/22 MOD/
TYP/RI DOT/19930825
OCA/31645326
MIS/
NIC/G629615373 DTE/19930825
RECORD IN NCIC
********** Validate This Record Modify This Record **********
********** Cancel This Record Clear This Record **********

CJIS MODEL VALIDATION PROCEDURES

The following validation procedures, developed pursuant to CJIS and NCIC policy requirements, must be followed exactly in order for an agency to properly validate its records. Failure to carefully execute these procedures could result in a costly civil, and possibly criminal, lawsuit.

For EACH record to be validated, you must do the following:

1. **FIND SOURCE DOCUMENTATION**

Pull the record's source document(s) (i.e., case file, physical warrant, arrest report, stolen vehicle report, etc.). ALL source documentation corresponding to EACH record being validated must be reviewed. Copies of CJIS and NCIC entries and/or worksheets are not proper source documentation.

Important: If source documentation cannot be found for the record, the record must be cancelled immediately from the CJIS and NCIC computer systems.

2. COMPARE THE RECORD WITH SOURCE DOCUMENTATION

Compare the information in the record with the information listed in the source document(s). You must check the following:

a.) **ACCURACY**: The information in the CJIS and NCIC records must match the information on the source document(s) exactly. Any error(s) in the CJIS and/or NCIC record must be corrected immediately using a modification message.

b.) **COMPLETENESS**: Each record entered into CJIS and NCIC must contain all available data. For example, such items such as Scars, Marks, Tattoos, Fingerprint Classification, and FBI Number must be added to a Wanted Person or Missing Person record when available.

If a case file contains information that has not been entered into the CJIS and NCIC record, you must modify the record so that it will reflect the additional information.

1.) It is suggested that, for wanted person records, the NCIC III file and the BOP file be checked for additional descriptors.

2.) For vehicle records, check with the RMV to confirm vehicle and license information.

IMPORTANT: Dental Records and Blood Type are CRITICAL components of a complete Missing Person entry.

3. OWNER, COURT, COMPLAINANT, DISTRICT ATTORNEY CONTACT

The next step in the validation process involves contacting the court that issued the warrant, the person that reported the vehicle or other property stolen, or the party that filed the missing person report. In the case of a warrant entered into NCIC, you must also contact the District Attorney in order to verify extradition (the exception to DA contact is a wanted person record which contains the code NOEX in the Remarks field). The underlying theory behind this process is that the appropriate owner, court, complainant, and DA are the ultimate sources for verifying the validity of a record. (**Note**: Warrant Management System (WMS) warrants that your agency has entered into NCIC can be validated by checking the warrant in the WMS.)

Contact can be made by:

1. Telephone call
2. Personal visit
3. Letter or postcard
4. Letter or memorandum to the courts or prosecutor

5. Letter, memorandum, or printout from the court or prosecutor identifying active warrants.

If contact cannot be made, a decision must be made by appropriate personnel whether or not to retain the record in the CJIS and NCIC computer systems.

IMPORTANT:

1.) If the District Attorney decides to narrow extradition limitations (e.g., New England States Only), then the Extradition Limitation (EXL) field must be modified immediately to reflect the new limits.

2.) If the District Attorney decides that extradition **will not** be authorized, then the EXL field must be modified immediately with the code of 4 for a felony offense or D for a misdemeanor offense.

3.) Extradition Limitations are as follows:

Felony Warrants

1 - Full Extradition unless otherwise noted in the MIS Field
2 - Limited Extradition see MIS Field (Requires data in the MIS Field)
3 - Extradition – Surround States Only
4 - No Extradition
5 - Extradition Arrangements Pending See MIS Field (Requires data in the MIS Field)
6 - Pending Extradition Determination

Section 32.2 Misdemeanor Warrants

A - Full Extradition
B - Limited Extradition See MIS Field (Requires data in the MIS Field)
C - Extradition – Surrounding States Only
D - No Extradition
E - Extradition Arrangements Pending See MIS Field (Requires data in the MIS Field)
F - Pending Extradition Determination

VALIDATING EACH RECORD

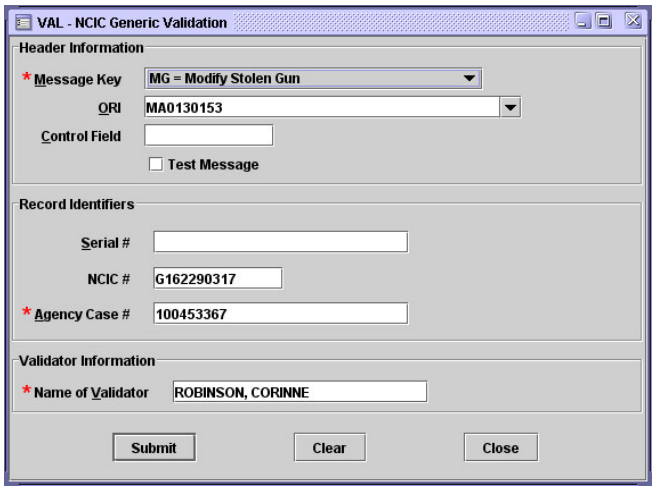
After reviewing the source documentation and after contact, or attempted contact, with the appropriate party(ies), the user must decide which of the following actions to take with the record:

- **Validate the Record** – The record is accurate, complete, and should remain in CJIS and NCIC.
- **Modify the Record** – The record must be modified due to the data being inaccurate and/or incomplete, or due to extradition limitations being changed.
- **Cancel the Record** – The record should have never been entered (e.g., the missing person report was falsely filed) or source documentation cannot be located.

- **Clear the Record** – The record should be removed as the stolen item has been recovered or wanted/missing person has been located.

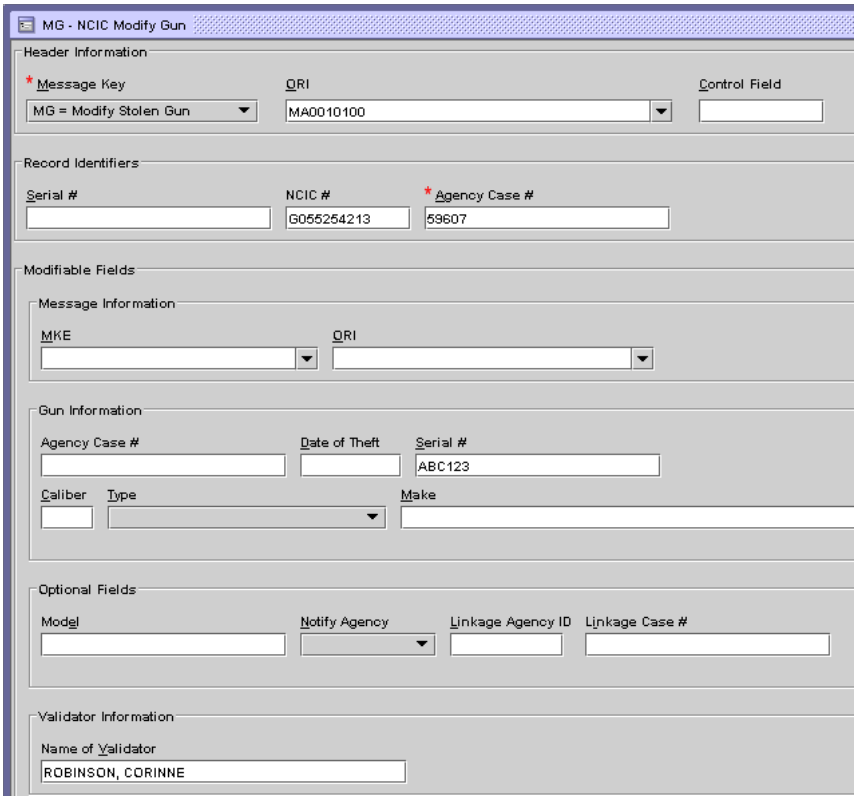
To complete the validation of each record:

1) Click the appropriate link for the action to be taken on the record. The associated form will be displayed with the Record Identifier fields populated and the Validator's Information displaying the username of the individual logged into the CJIS Messenger application. Note that the forms to Cancel and Clear records do not include Validator Information.



2) Click the Submit Button. The record is validated and the user may move on to the next record or file as necessary.

IMPORTANT: If modifying the record, enter the correct data to fix any errors, or add additional information to the record as required AND enter the Name of Validator information (Last name, First Name). See example below:

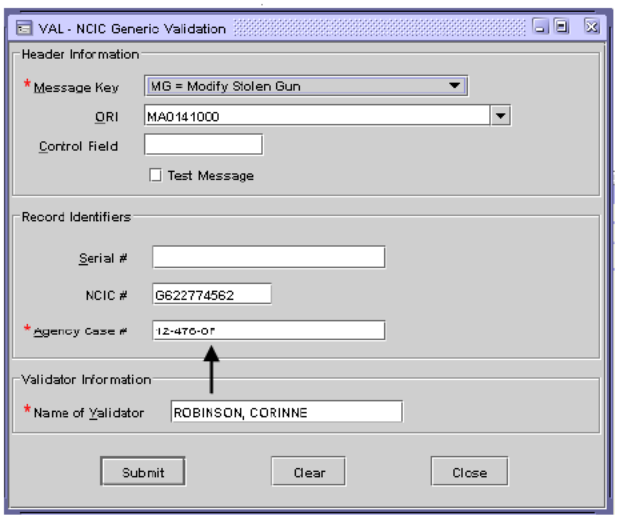


NOTE: The QVAL summary reduces each time a record is validated. When there are no records remaining to validate, the QVAL will return a notice like the following:

NO {MONTH} RECORDS PENDING FOR VALIDATION BY AGENCY ORI/MAMSP0000

RECORD VALIDATION TIPS:

1) NCIC 2000 may translate the letter O to a 0. If the VAL – NCIC Generic Validation pre-populated Agency Case # information does not match the record's OCA # exactly, the record will not validate. A user may get a record validated message from MACJIS while NCIC will return a Reject Not on File Message.



To ensure that the validation is successful, change the zero (0) to the Letter O and click submit.

SECURITY AWARENESS TRAINING

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. Local Agency Security Officers (LASO) require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems. DCJIS utilizes Level One Security Awareness Training for all personnel with unescorted access where CJI is being accessed and/or process to include custodians. Level Four Security Awareness Training is for all personnel with physical and logical access to CJI and for all Information Technology personnel.

Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The agency head may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior regarding being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

Level Four Security Awareness Training

In addition to the above, the following topics at a minimum shall be addressed as baseline security awareness training for all authorized personnel with access to CJI both physical and logical, and Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through

destruction.

3. Proper handling and marking of CJI.

4. Threats, vulnerabilities, and risks associated with handling of CJI.

5. Social engineering.

6. Dissemination and destruction.

7. Rules that describe responsibilities and expected behavior regarding information system usage.

8. Password usage and management—including creation, frequency of changes, and protection.

9. Protection from viruses, worms, Trojan horses, and other malicious code.

10. Unknown e-mail/attachments.

11. Web usage—allowed versus prohibited; monitoring of user activity.

12. Spam.

13. Physical Security—increases in risks to systems and data.

14. Handheld device security issues—address both physical and wireless security issues.

15. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.

16. Laptop security—address both physical and information security issues.

17. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).

18. Access control issues—address least privilege and separation of duties.

19. Individual accountability—explain what this means in the agency.

20. Use of acknowledgement statements—passwords, access to systems and data, personal use, and gain.

21. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.

22. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.

23. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

24. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.

25. Data backup and storage—centralized or decentralized approach.

26. Timely application of system patches—part of configuration management.

27. Access control measures.

28. Network infrastructure protection measures.

LASO TRAINING

Local Agency Security Officer (LASO) training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the local agency.

SYSTEM AUDITING AND ACCOUNTABILITY

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

Events

1. Successful and unsuccessful system log-on attempts.

2. Successful and unsuccessful attempts to use:
   a. access permission on a user account, file, directory or other system resource;
   b. create permission on a user account, file, directory or other system resource;
   c. write permission on a user account, file, directory or other system resource;
   d. delete permission on a user account, file, directory or other system resource;
   e. change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change account passwords.

4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).

5. Successful and unsuccessful attempts for users to:
   a. access the audit log file;
   b. modify the audit log file;
   c. destroy the audit log file.

Content

The following content shall be included with every audited event:

1. Date and time of the event.

2. The component of the information system (e.g., hardware or software component) where the event occurred. (e.g., software component, hardware

3. Type of event.

4. User/subject identity.

5. Outcome (success or failure) of the event.

Response to Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion, and unauthorized access.

Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information - The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Agency Administrator (AA) - An individual located within an agency that is ultimately responsible for security and compliance requirements.

Administrative Messages (AM) - A secure and documentable means of interagency communication. An AM may be used for any type of official law enforcement or public safety purpose as approved by Nlets and NCIC.

Assistant Terminal Agency Coordinator (ATAC) - An individual located within an agency designated to assist the terminal agency coordinator as liaison between the agency and the CSA.

Authorized Personnel/Criminal Justice Practitioner - A non-sworn or non-terminal operator that could receive or view hard copy CJIS/NCIC record information.

AUTHORIZED RECIPIENT (Civil Accounts) - (1) A non-governmental entity authorized by federal statute or federal executive order to receive CHRI for non-criminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for non-criminal justice purposes.

Authorized User/personnel - An individual, or group of individuals, who have been appropriately vetted (national fingerprint-based record check, a wants/warrant check and received appropriate training) and have been granted access to CJI.

CJIS Security Officer (CSO) - An individual located within the CSA responsible for the administration of CJIS for the CSA.

CJIS Security Policy - The FBI CJIS Security Policy document as published by the FBI ISO.

CJIS System Agency (CSA) - A state criminal justice agency providing access to its criminal justice users with respect to CJIS data. There can only be one CSA per state.

Confidentiality - The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor **and/or Vendor** - A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice or a Non-Criminal Justice Agency.

Criminal History Record Information (CHRI) - A subset of CJI. Any notations or other Written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Information (CJI) - Criminal Justice Information is the abstract term used to refer to all the DCJIS and FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the DCJIS and FBI CJIS-provided data necessary for civil agencies to perform their mission; including but not limited to data used to make hiring decisions.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division Responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Department of Criminal Justice Information System (DCJIS) - The primary function of the Nevada Criminal Justice Information System is to provide an efficient and effective system for the expeditious exchange of criminal justice or related information.

Direct Access - (1) Having the authority to access systems managed by DCJIS and the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by DCJIS and the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination -Disclosing records of criminal history or the absence of records of criminal history to a person or agency outside the organization which has control of the information.

Escorting - An unauthorized person in a physically secure area must be escorted by a person who is sufficiently familiar with the equipment in the area and the tasks being performed. The escort must be able to identify unauthorized act and alert security personnel. If the escort does not have this set of knowledge and skills, then the person cannot be an escort.

FBI - Federal Bureau of Investigation

Information Security Officer (ISO) - An individual designated by the CSO who has the responsibilities to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversee the governance of security operations and establishes information security training and awareness programs. The ISO interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Interstate Identification Index (III) - The CJIS service that manages automated submission and requests for CHRI that is warehoused after the submission of fingerprint information. Subsequent requests are directed to the originating state as needed.

Law Enforcement National Data Exchange (N-DEx) - FBI CJIS division system providing law enforcement agencies with a shared investigative tool.

Local Agency Security Officer (LASO) - A point-of-contact designated as the liaison between their agency and the ISO who has access to the DCJIS network and provides any needed technical systems assistance to help assure the confidentiality, integrity, and availability of criminal justice information on the network.

National Crime Information Center (NCIC) - FBI information system which stores CJI which can be queried by appropriate Federal, state and local law enforcement, criminal justice and certain noncriminal justice agencies.

Nlets - The International Justice and Public Safety Network.

Non-Terminal Agency (NTA) - An agency having access to DCJIS/NCIC information through a terminal agency.

Non-Terminal Agency Coordinator - An individual located within an agency designated as the liaison between his or her agency and the CSA. The TAC administers DCJIS/CJIS systems programs within the local agency and oversees the agency's compliance with those policies.

Originating Agency Identifier (ORI) - A unique alpha numerical

identifier authorized by the CSA.

Physically Secure Location - A facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Secondary Dissemination - The release of CHRI from one agency to an authorized recipient agency when the recipient agency's ORI was not used to run the transaction.

Terminal Agency (TA) - An agency that has direct computer access to the DCJIS/NCIC system.

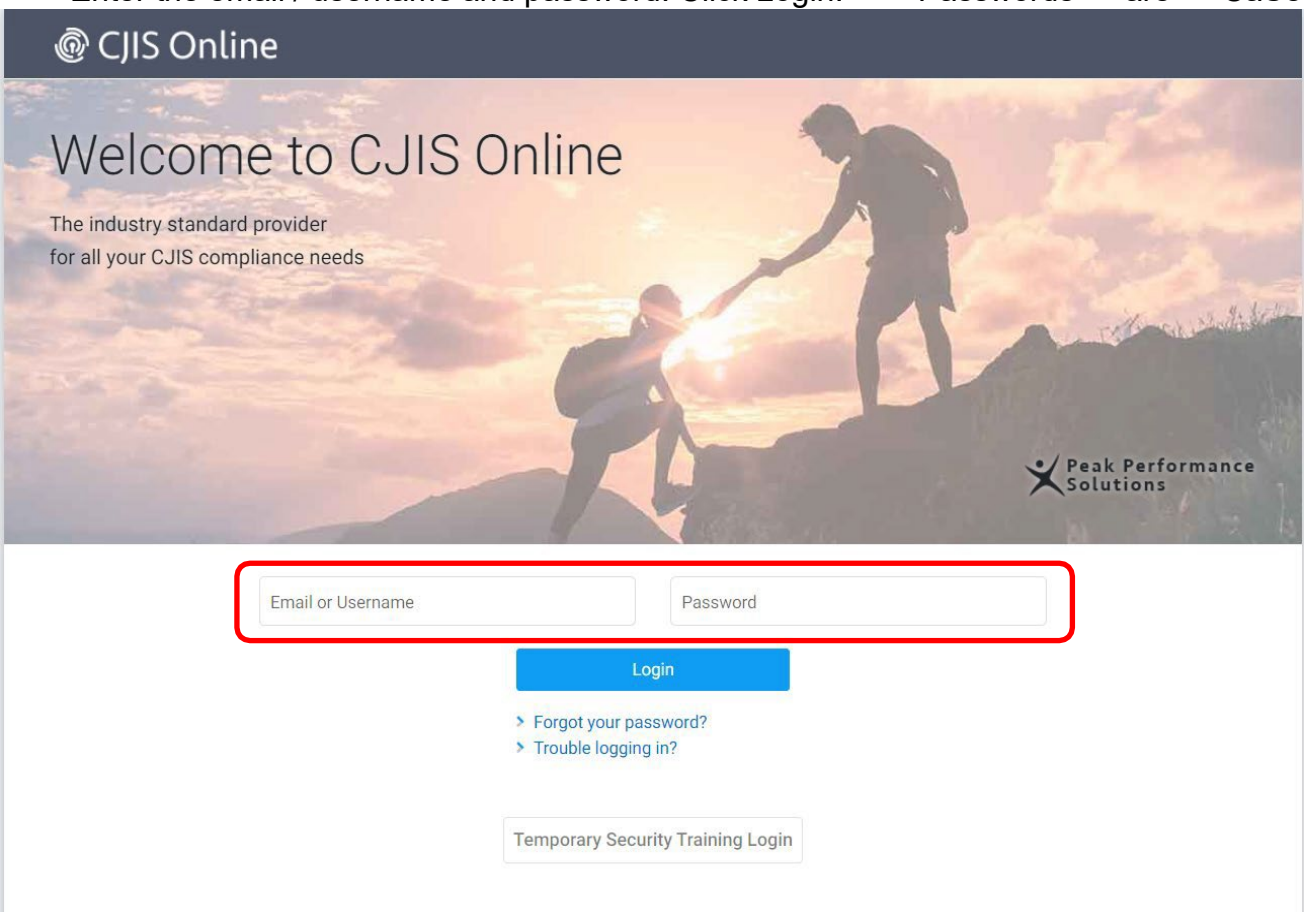
Terminal Agency Coordinator (TAC) - An individual located within an agency designated as the liaison between his or her agency and the CSA. The TAC administers DCJIS/CJIS systems Programs within the local agency and oversees the agency's compliance with those policies.

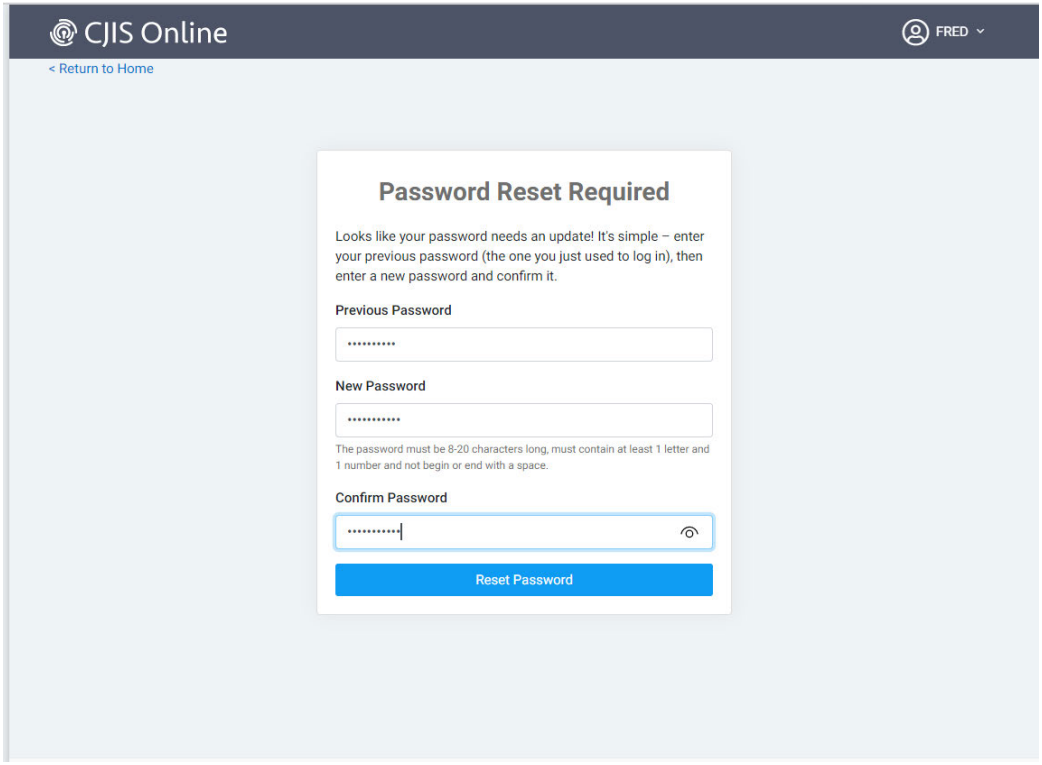
Terminal Operator - An individual, that transmits, receives and coordinates information through direct communication to the DCJIS system (DCJIS, NCIC, and Nlets in compliance with state and federal regulations.

APPENDIX B **CJIS ONLINE**

https://www.cjisonline.com

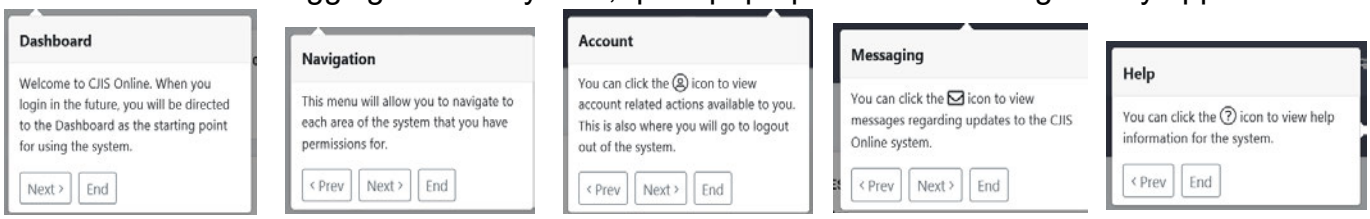
Enter the email / username and password. Click Login. Passwords are CaSe SeNsiTiVe.

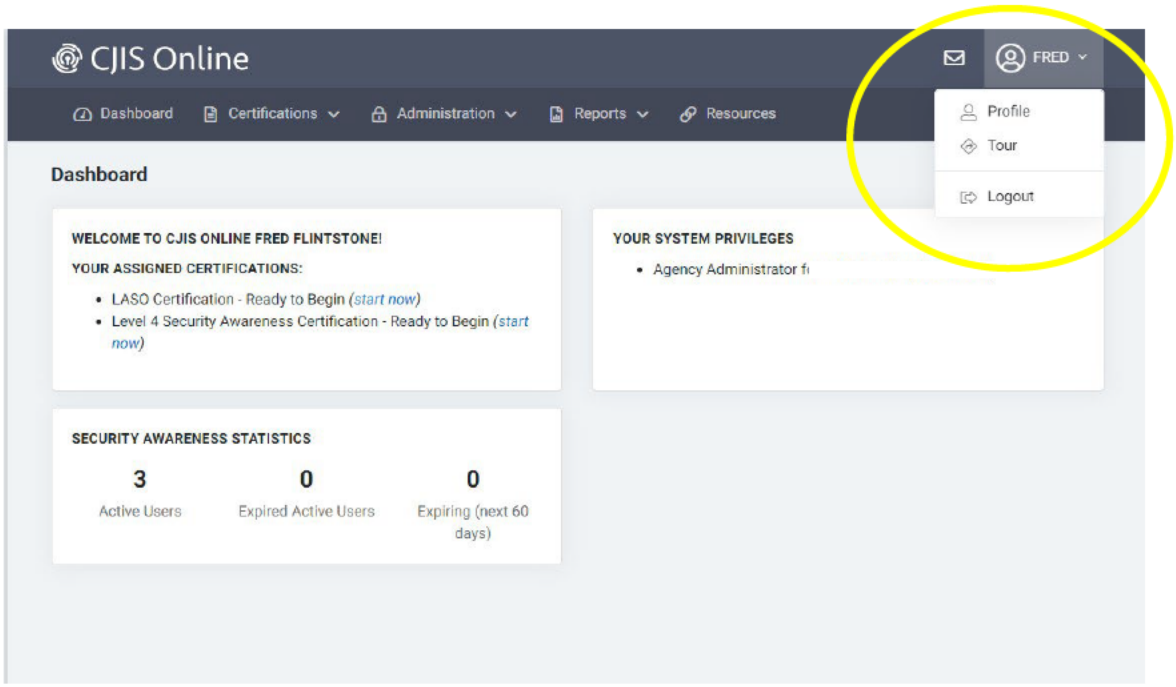




First time sign in, one may be prompted to change their password.
If needed, create a new password to continue. The fields are CaSe SeNsiTiVe.

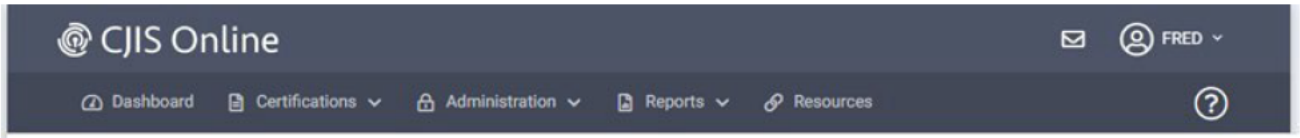
First time logging into the system, quick pop-up notes or messages may appear.





This is the main Dashboard providing quick stats. In the top right corner, click on the chevron symbol next to your name to view the pop-up notes again, **Edit** your Profile, view certificate details and history, and use **Logout** to leave the system.

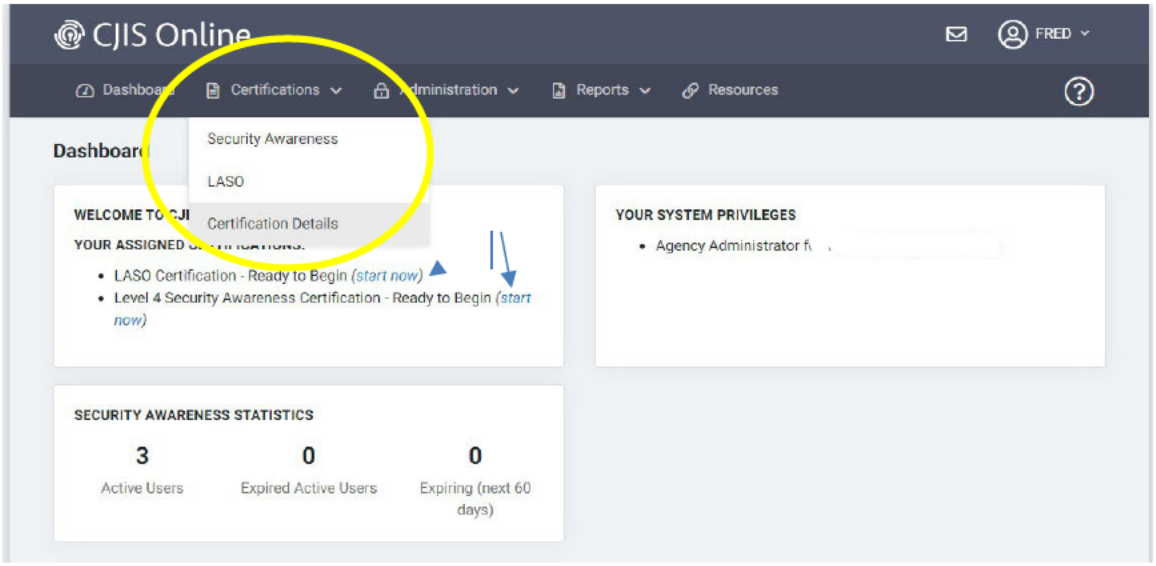
The **Envelope** contains messages from the application.



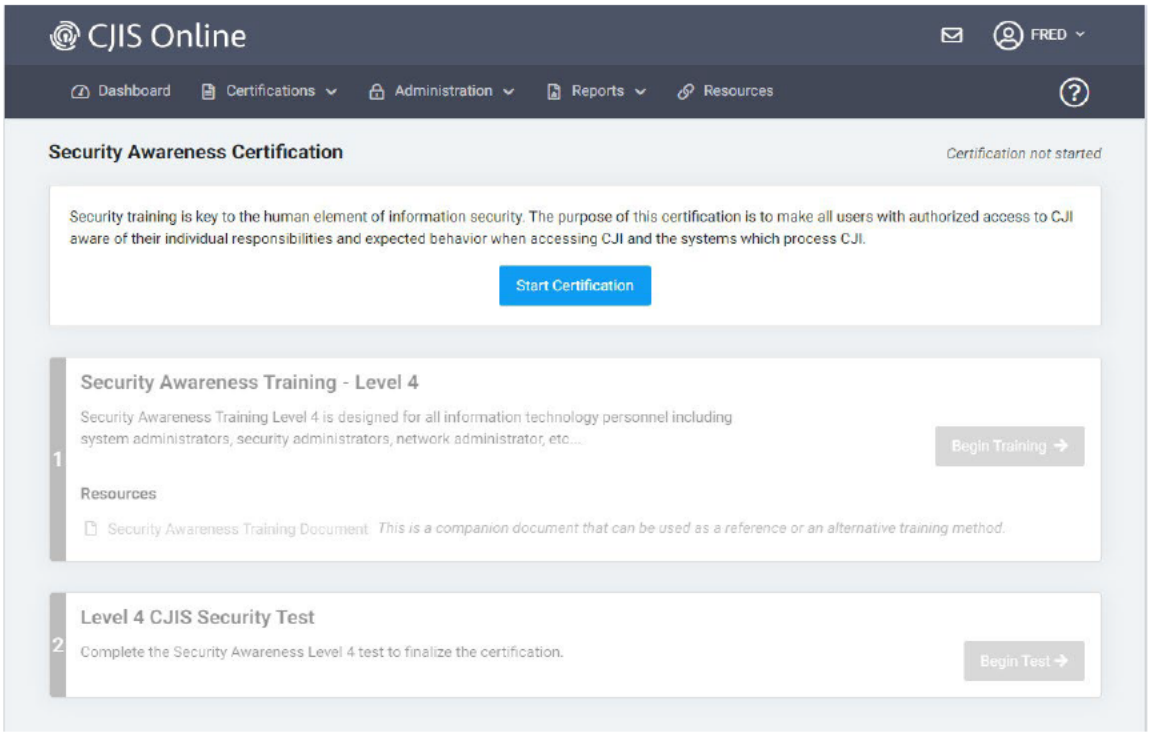
The task bar contains the main **Dashboard**, **Certifications** Menu, **Administration** Menu, **Reports** Menu,
Resources Menu and **?** for additional help.

Let's get started!

Explore the Certifications Menu



From this menu quickly see Security Awareness, LASO and Certification Details. One can start Training and Testing by clicking on the **Start Certification** button like below from the Certifications Menu or from blue links on the main Dashboard.

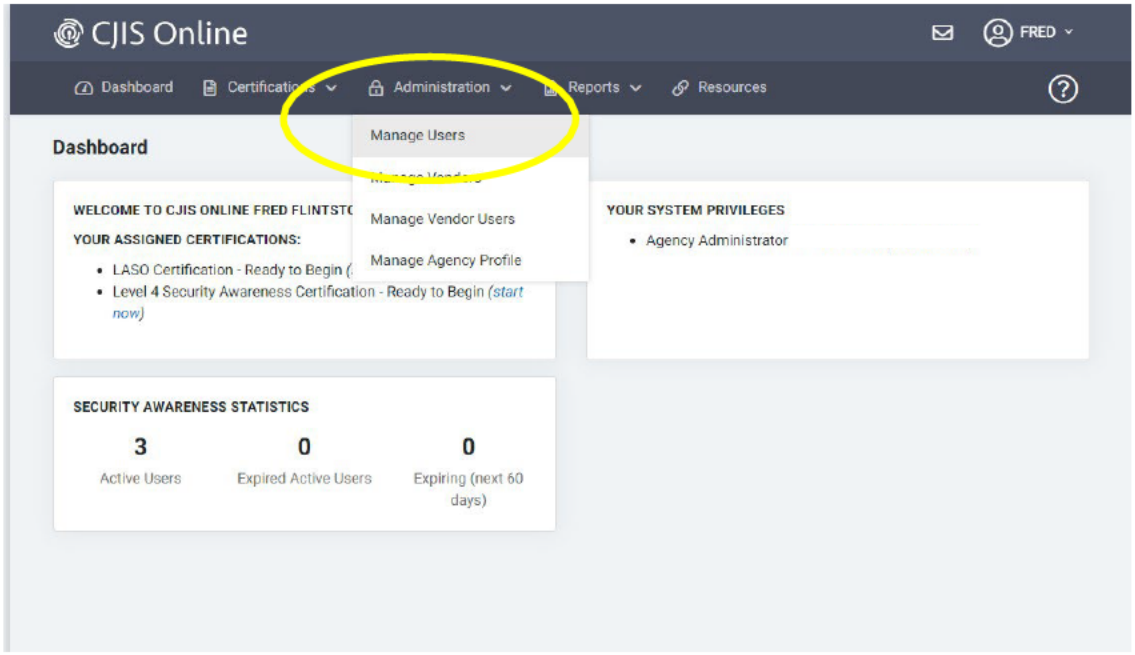


Sample of Security Awareness Certification page from the Certifications

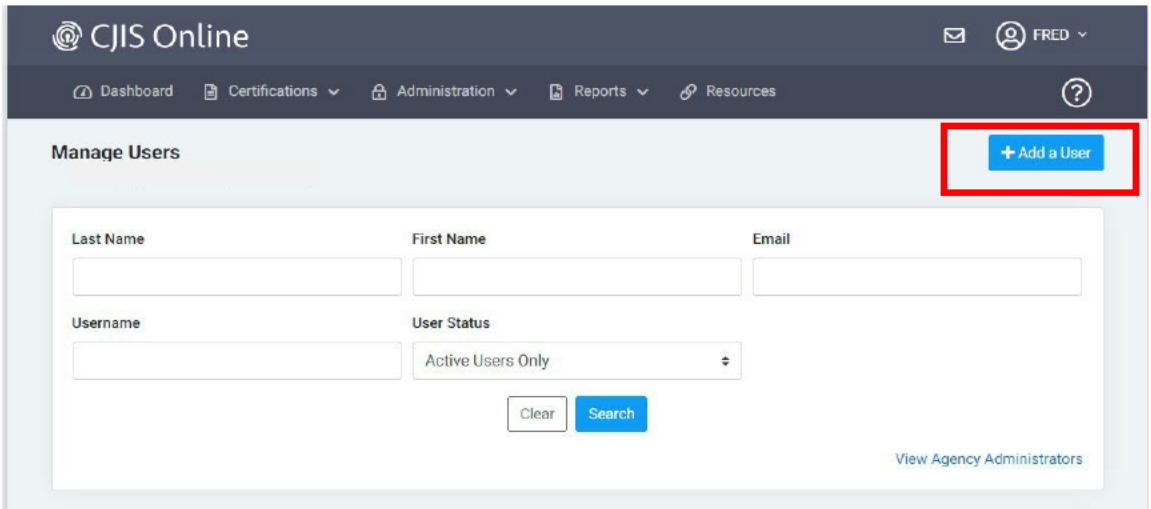
Menu. An individual's training may appear differently per the varying training levels assigned by the Local Admin.

Accounts – adding new Local AGENCY users and updating user account information

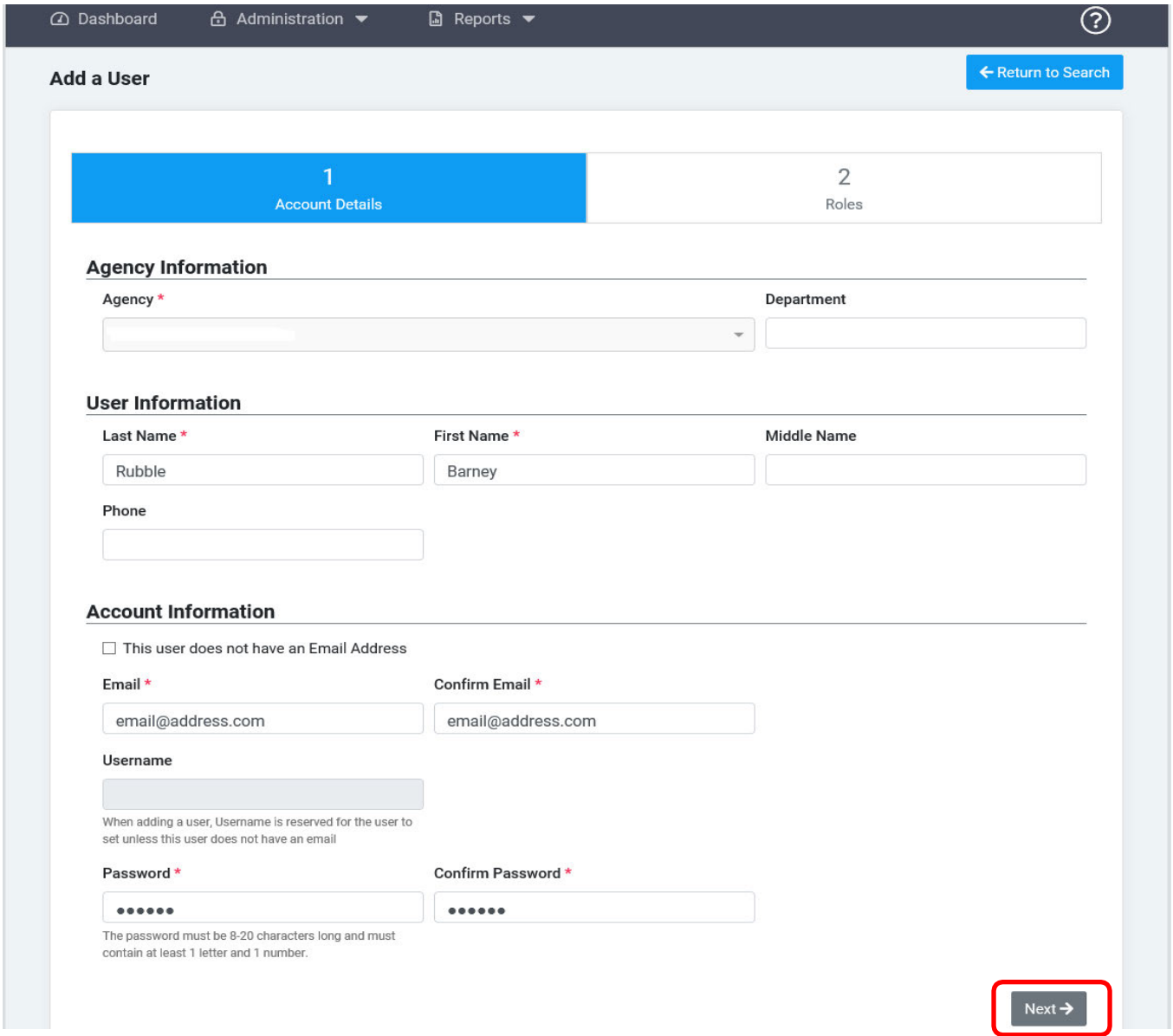
Click on **Administration** then **Manage Users**.



To Add a New User Account



Click on **+Add a User** button.



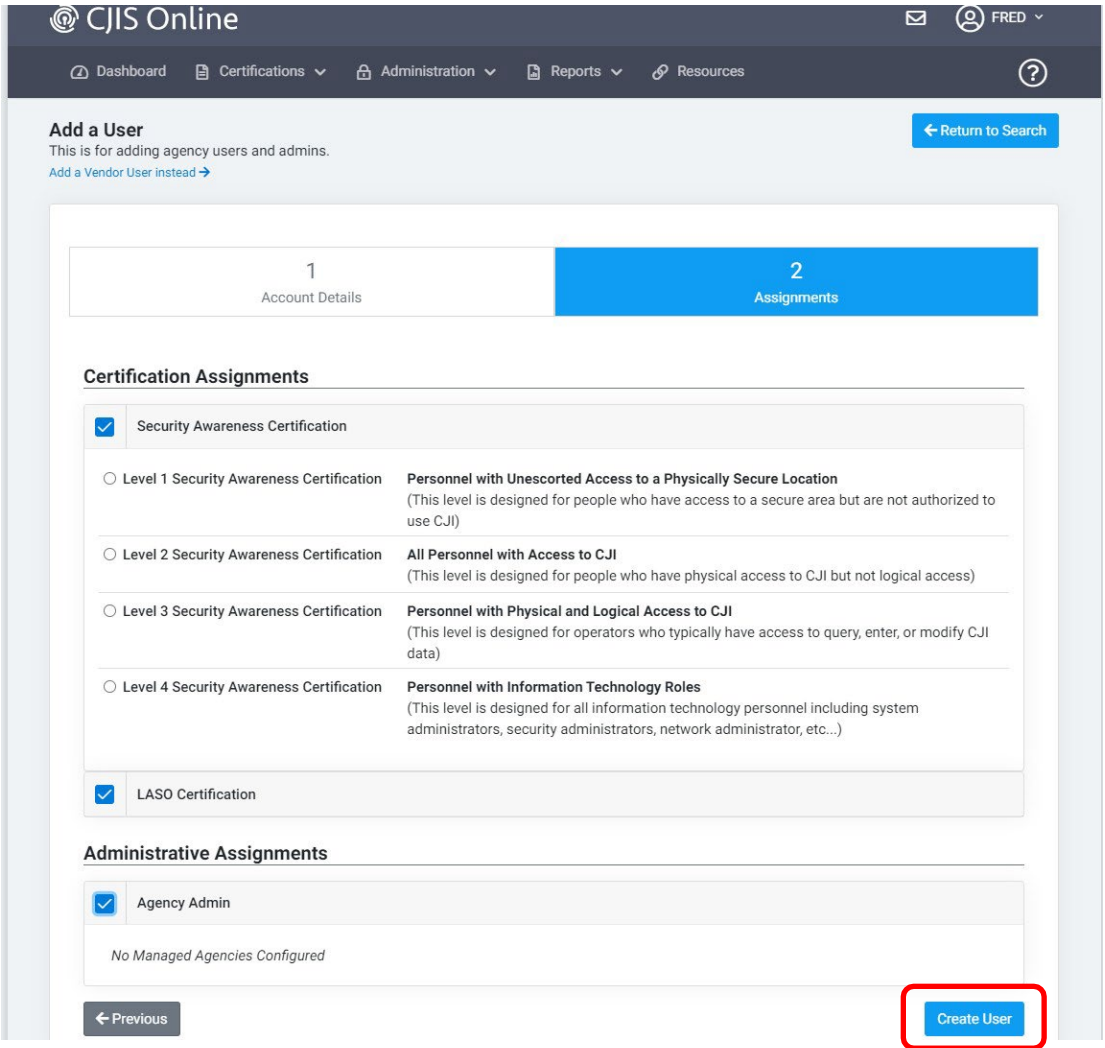
All fields with an asterisk * are required. The ORI field should auto populate.
Enter **Last Name**, **First Name**, **Email**, **Confirm Email,** then enter and confirm an initial **password**.

If the individual does not have an email address, check the box next to “This user does not have an Email Address” then enter a unique **Username** instead. The individual *cannot* be notified when their training is expiring without an email address entered.

Your admin account allows you access to change passwords and edit fields on agency user and vendor user accounts. You may assign more Admin accounts and add LASO Training to accounts. Click **Next** when ready**.**

Note: Please remember the password you entered to provide to the end user so they may sign on. You will need to let the user know their initial password. Account information cannot be

deleted; only made inactive. Use caution when creating new accounts when personnel transferred in from other agencies, please contact us to check and move any existing records before creating new accounts as individuals may have completed training previously.



Click on the appropriate Security Awareness Training level needed. LASO and Agency Admin access can be added
to the user account on this screen. Click **Create User** when ready.
A quick pop-up message appears when the account was successfully created.

Security Awareness Training level examples:
Level 1 - personnel coming into the secured area – maintenance, admin
Level 4 – personnel with direct access to CJIS and/or have unescorted access where CJI is processed - personnel working on network and computers – internal/city/government IT staff

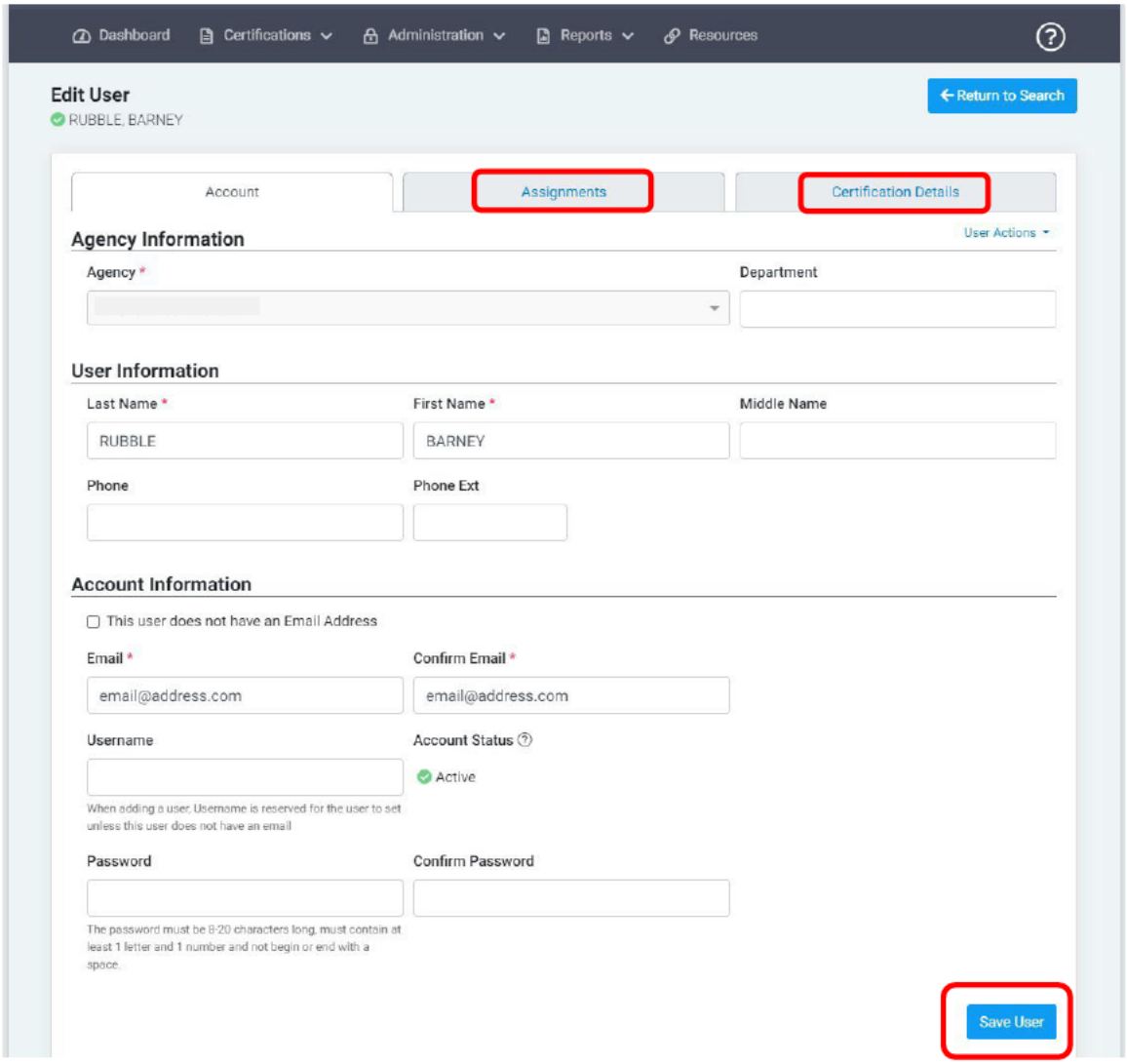
Level 2 and 3 – not used

LASO – Local Agency Security Officer Training – person knowledgeable in computer security or network intricacies, account handling, system access given, incident handling - city/government IT staff, TAC

Agency Admin – Assign additional admin accounts for the agency. Admin accounts

can add more accounts, change passwords, and edit fields on agency user and vendor user accounts. Account information cannot be deleted; only made inactive.

This screen returns for further user account editing if needed.



To edit the existing account created, click on **Assignments** to change training level, add LASO or Admin access.
Choose **Certification Details** to view testing records, then click the **>** greater than symbol on the certification name line to view/reprint certificates. Note: the Background checks section on the Certification Details tab is **not** required to be filled in. When done editing click **Save User.**

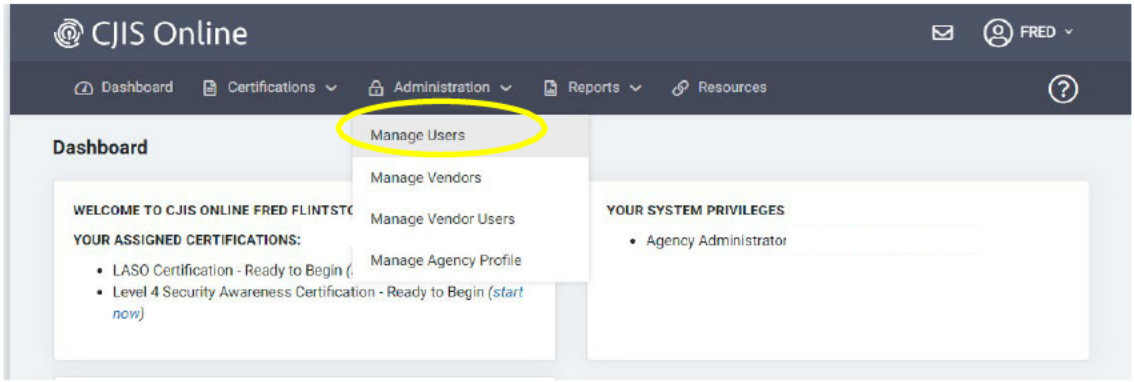
To add another new account, click on **+Add**

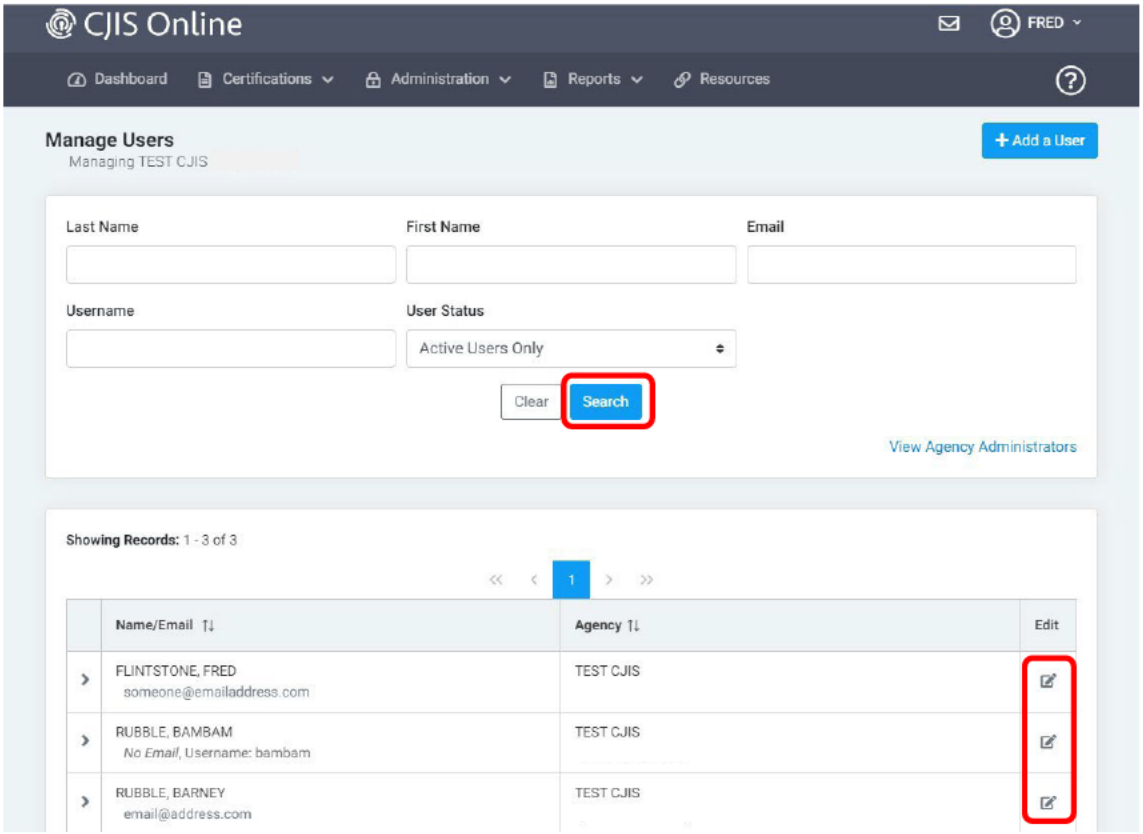
Another User button. To find an existing user to

edit, click <- **Return to Search** button.

To Search for Agency User Account

Click on **Administration** then **Manage Users**.



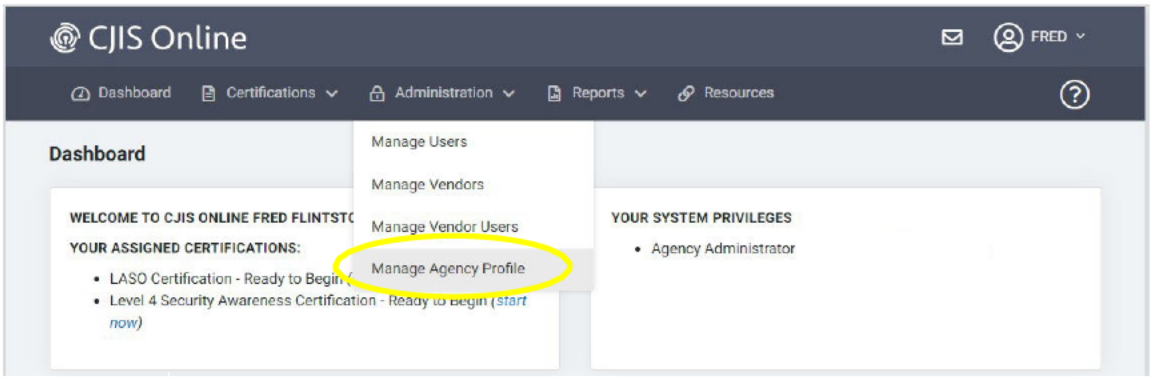


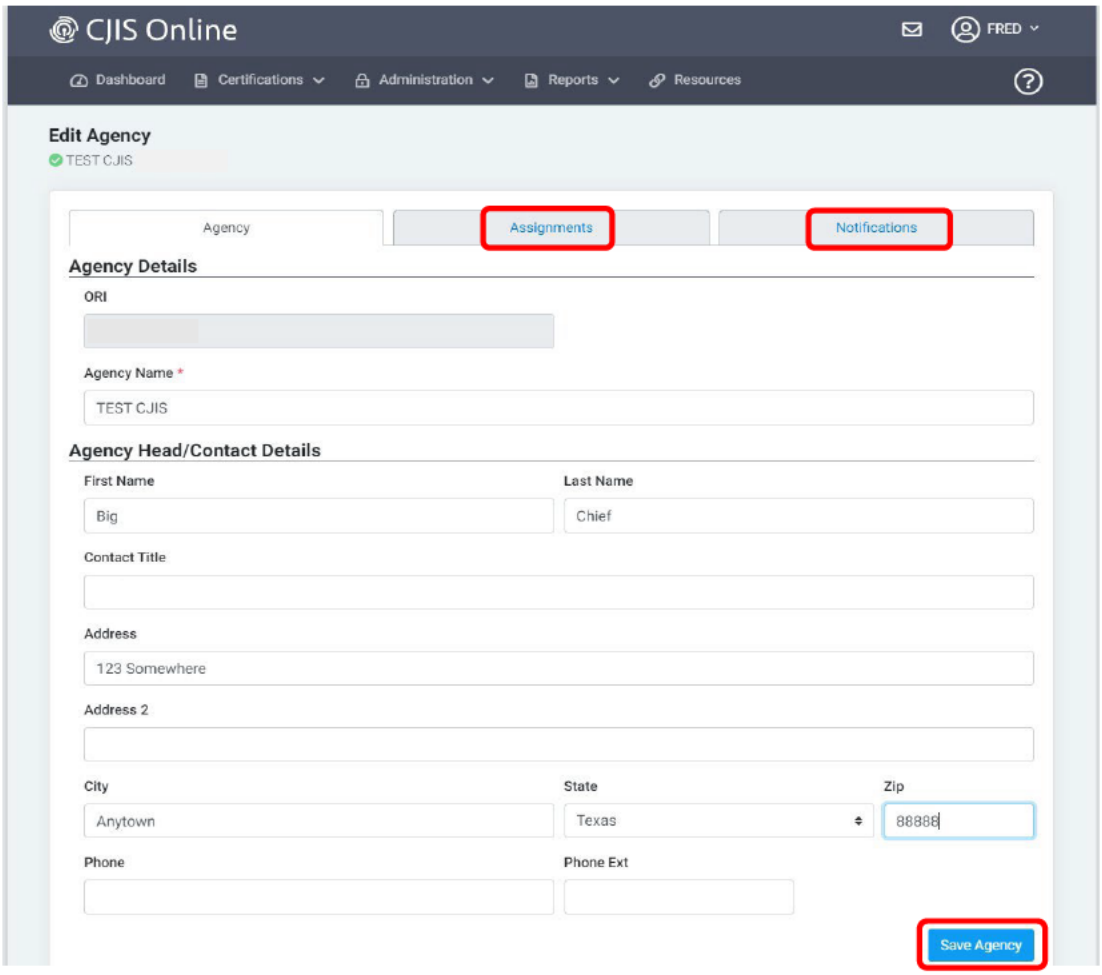
You can search by name, email address, user status (Active/Inactive/All) or role. Enter the search criteria and click on **Search** button.

Find the User account and click on Edit pencil & paper icon to edit the account. Remember to click **Save User** when done editing the account.

To Edit Your Agency Information

Click on **Administration** then **Manage Agency Profile**





Enter any changes needed. Fields with an

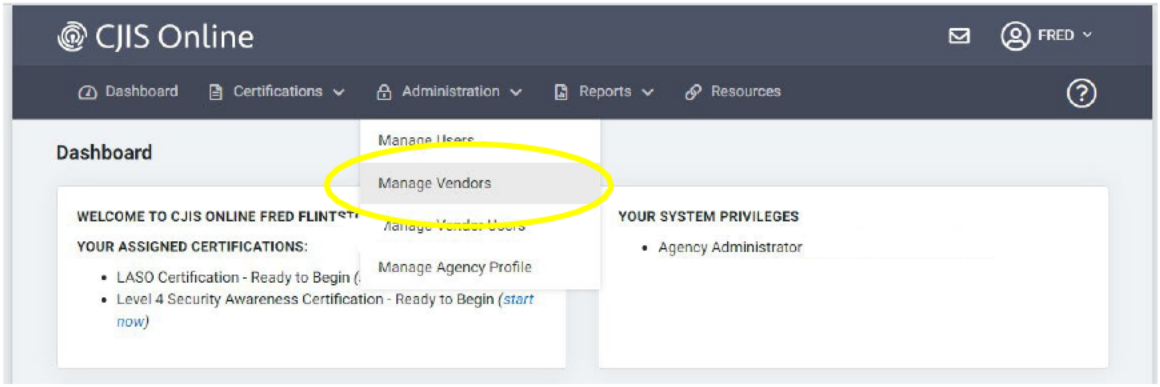
asterisk * are required. When done click **Save**

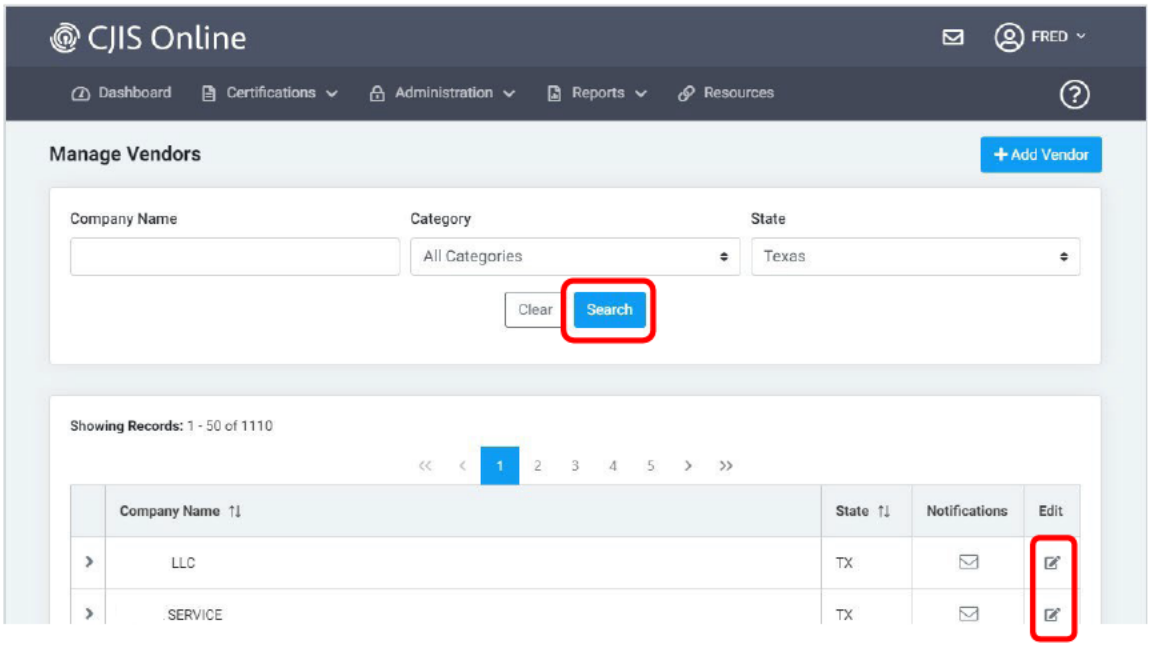
Agency.

From this screen you can choose to Edit Admin and LASO roles on the Assignments tab and choose other accounts to receive email notices on the Notifications tab.

To Search Vendor Records

Click on **Administration** then **Manage Vendors.**



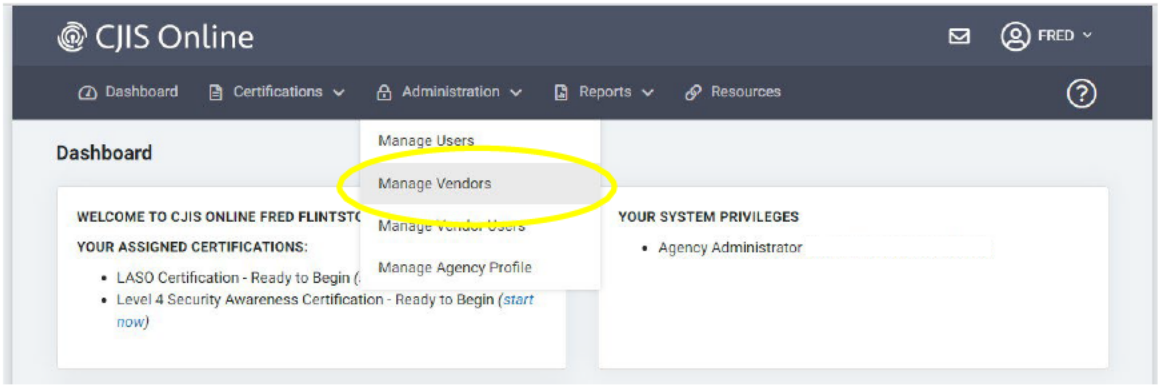


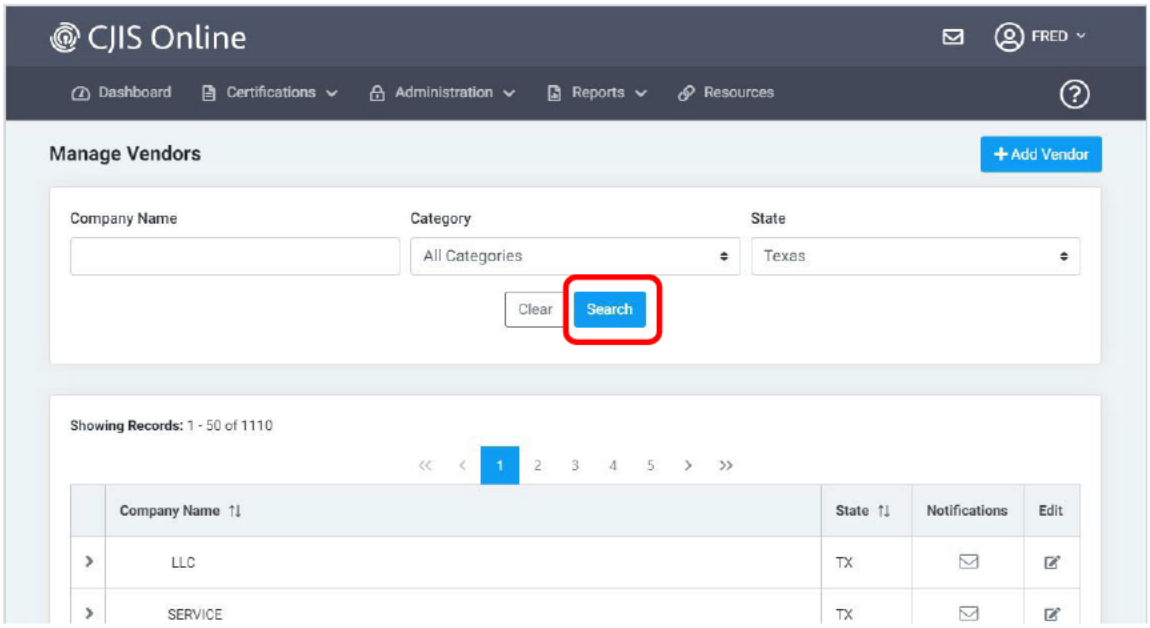
You can search by Company name, category and/or state. Click **Search**.

Find the Company Name and click on Edit pencil & paper icon to edit the account. Remember to save any changes when done.

To Add a Vendor

! Only after you have extensively searched by company name (full or partial name) AND have searched by a known individual employed by the vendor, you may enter a new vendor record. Do NOT enter vendor employees as your agency employees as other agencies may use the same vendors. There is a different method to add Vendor Users.

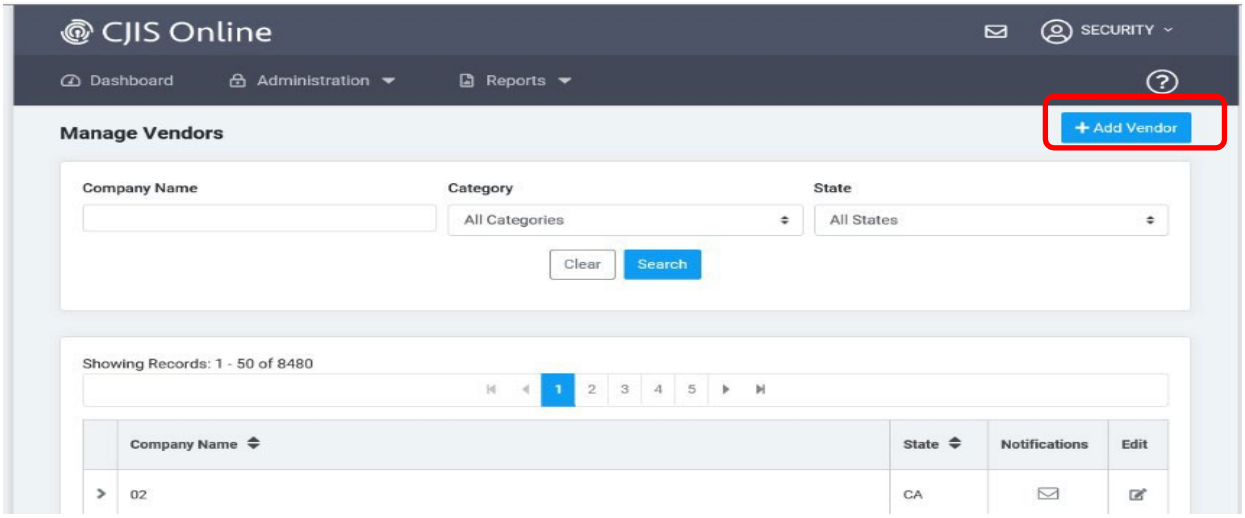




Enter a **Company Name** and click **Search**.
If no records are found, but you know the individual worked for this vendor in the past or works for another agency, Search for *Vendor User* Account instead and check company name spelling in user account settings Go to the section on *Vendor User Accounts* to search for an individual user account. The company name could have changed or is spelled differently.

If no results are found by username search, then you may proceed to

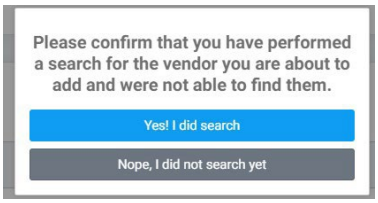
add a new Vendor.Note: If error message appears for email address is in use, this means the record exists.

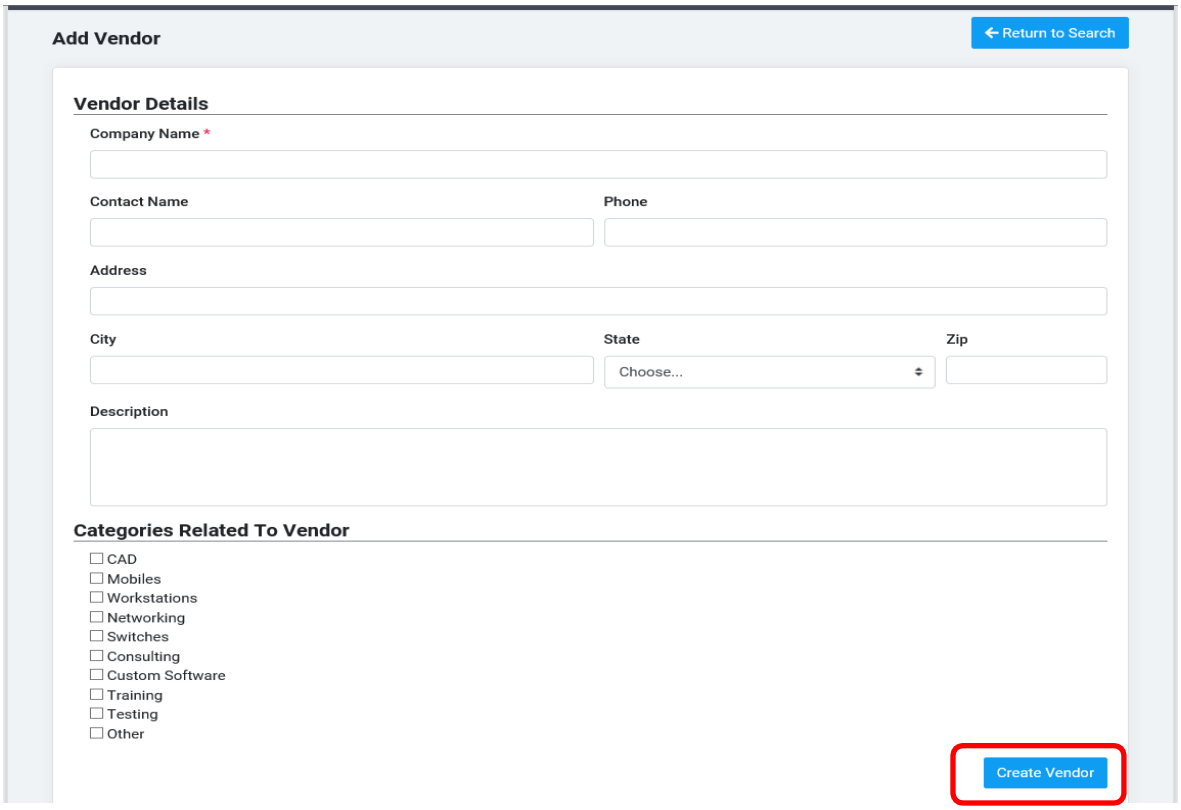


Click on **+Add Vendor.**

A prompt may appear to validate you have searched before entering a new record. Choose Yes or Nope to confirm.

You will not have the ability to disable or remove a vendor record if created in error.

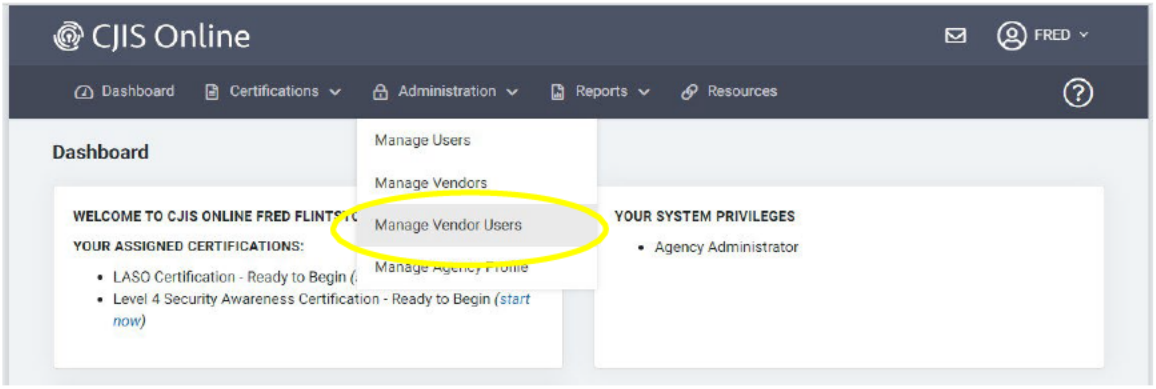




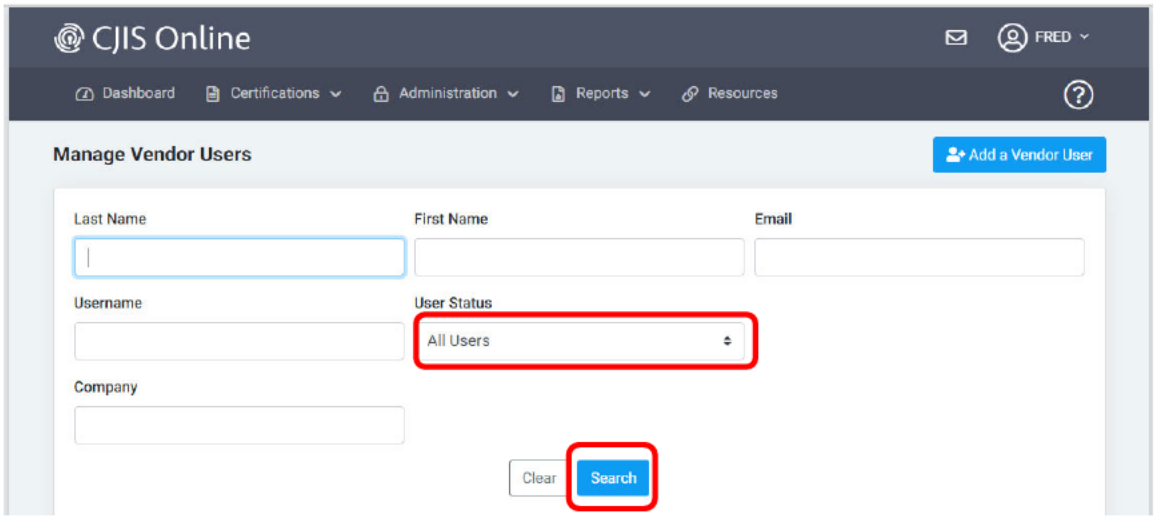
Enter a company name and pertinent information. Fields with an asterisk * are required. Click **Create Vendor.**

Vendor User Accounts – adding new VENDOR users and updating information

Click on **Administration** then **Manage Vendor Users.**



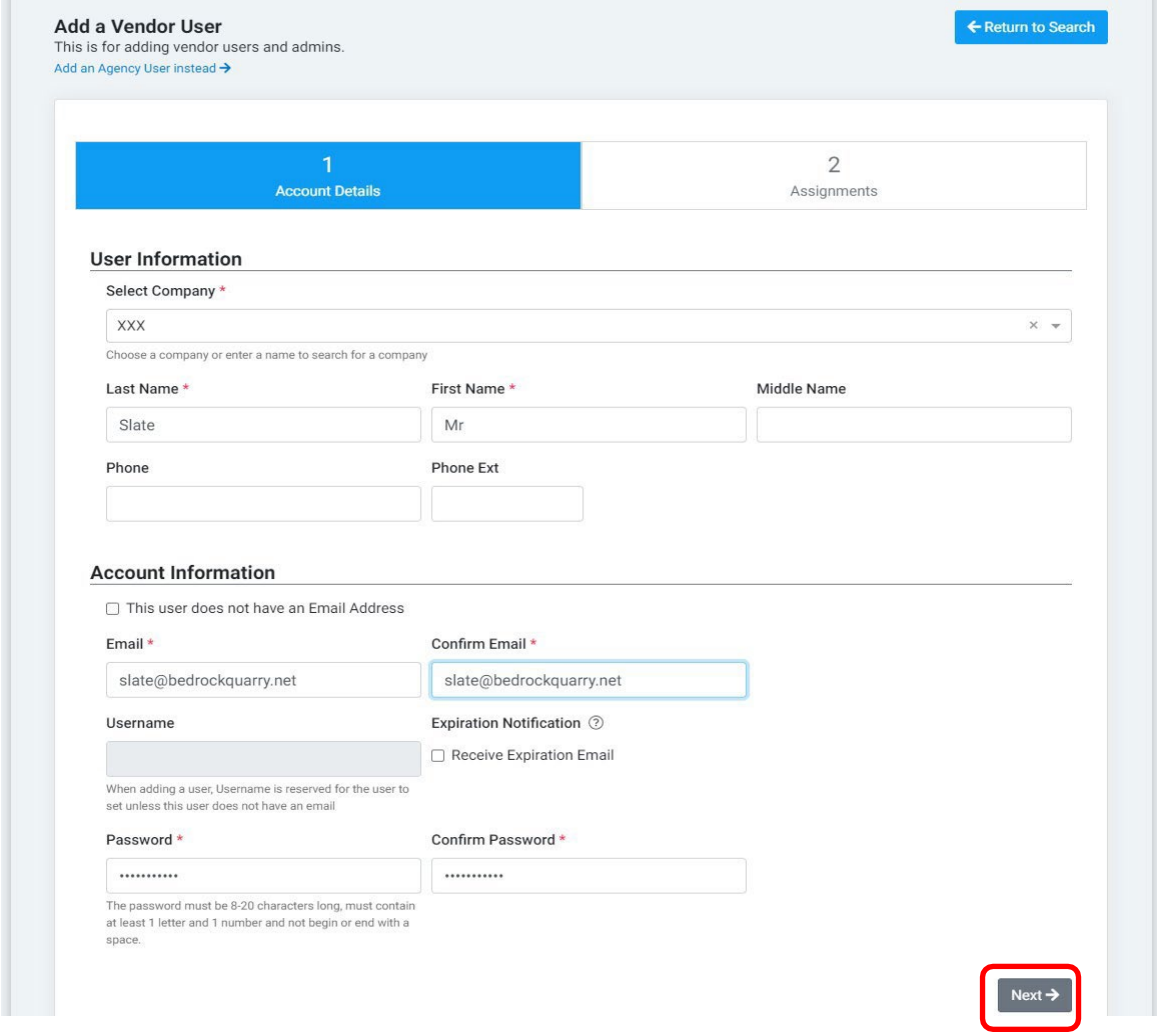
First, find if the user account exists!



Enter the individual's **Last Name**, **email** or **Company**. Choose *User Status* ***All Users*** and click **Search.**

If you do not see the record on the screen bottom, you may proceed to enter a new account. If there is a user record, the account exists.

Click on **+Add a Vendor User** button.

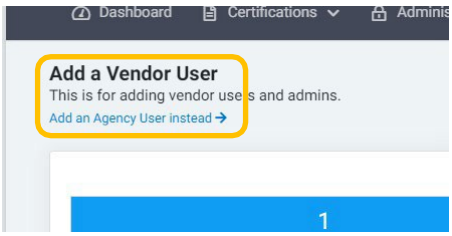


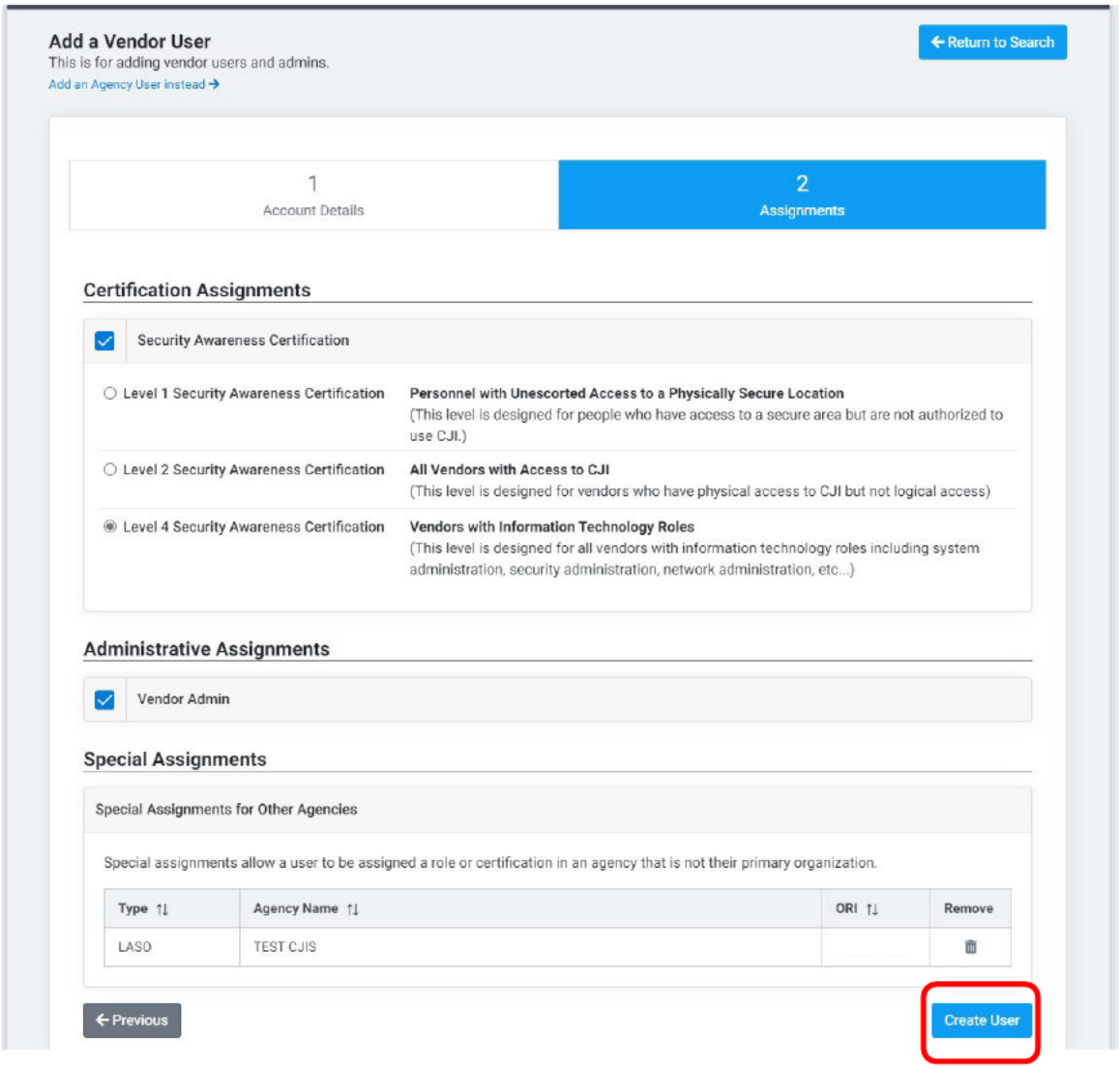
All fields with an asterisk * are required. Enter/search in the **Select Company** field. Enter **Last Name**, **First Name**, **Email, Confirm Email,** then enter and confirm an initial **password**.

If the individual does not have an email address, check the box next to “This user does not have an Email Address” then enter a unique **Username** instead. The person will *not* be notified when their training is expiring without an email

address entered. Click **Next.**

Note: Receiving a message account already exists means, the email is already in use and one will need to
Search again. Please remember the password you entered to provide to the end user so they may sign on. You will need to let the user know their initial password. If you really needed to add an *Agency User Account instead* of a vendor user, in the top left corner, choose ‘Add an Agency User instead-> ’ and the correct screen will appear.


Dashboard
Certifications
Add a Vendor User
This is for adding vendor use s and admins.
Add an Agency User instead
1



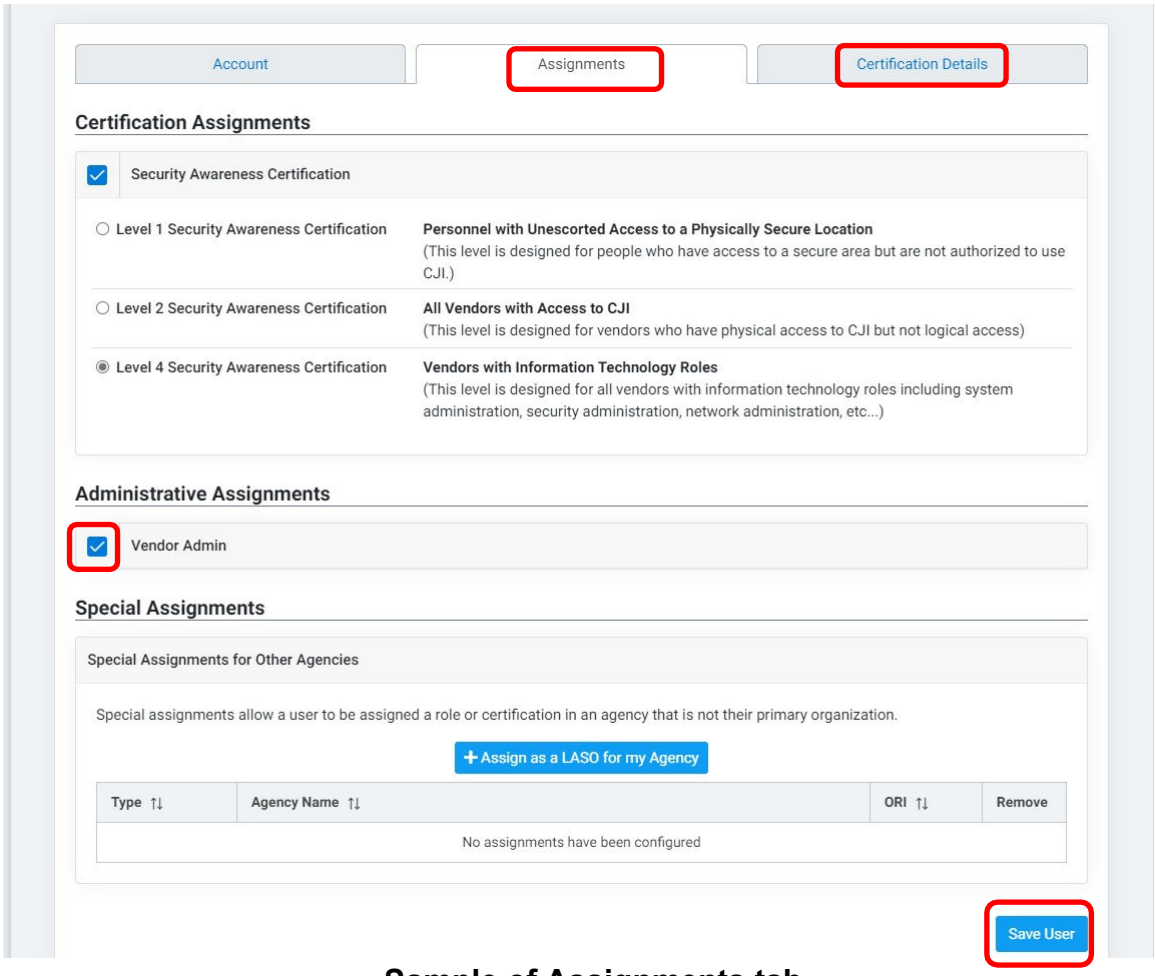
For IT/CAD/RMS/software/network/computer/remote access/ related vendors, choose **Level 4 CJIS Security Training**.

If the individual will have Admin Access to enter and administer their own employees, click on Vendor Admin Access.

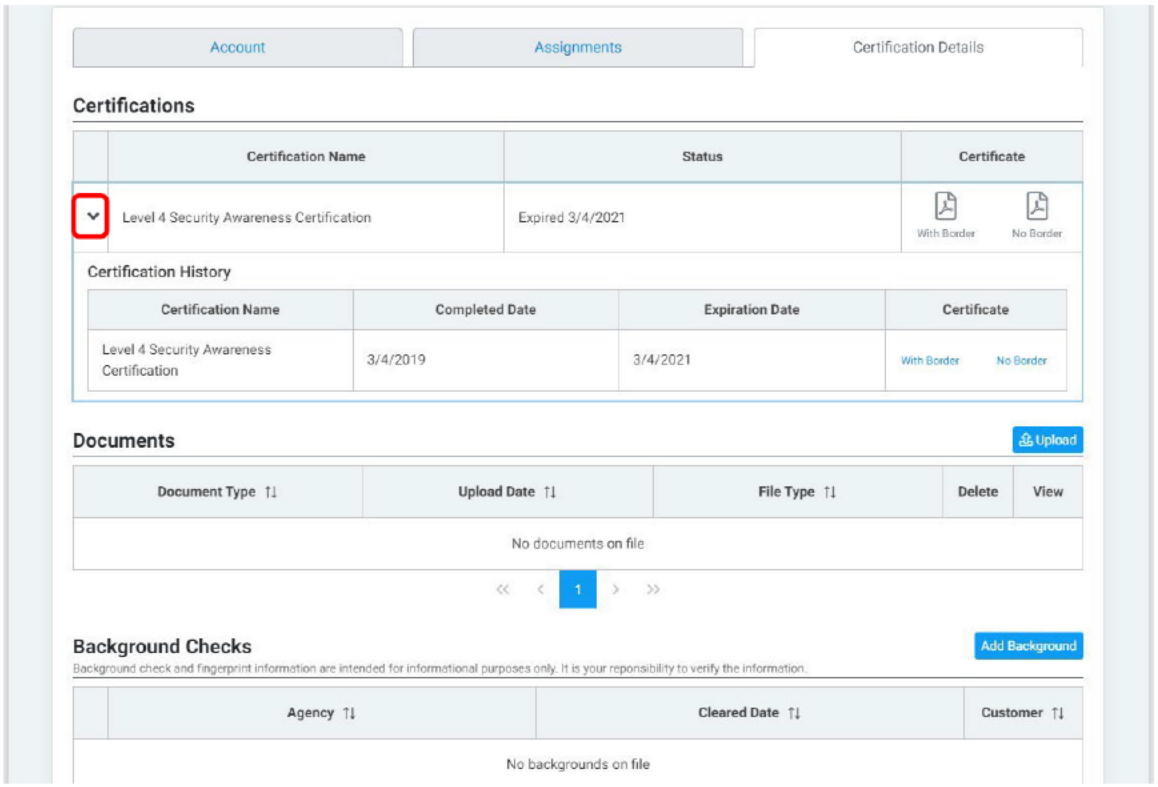
Click **Create User**. A quick pop-up message appears with the account was successfully created.

Vendors may have multiple admins. The agency can add the vendor user accounts or delegate this to the vendor company by creating them a Vendor Admin account, so the vendor may enter their own employees.

A summary of the account created appears for any final edits. Click on the **Assignments** tab or **Certification Details** tab to review this information too. Click **Save User** when done.



Sample of Assignments tab

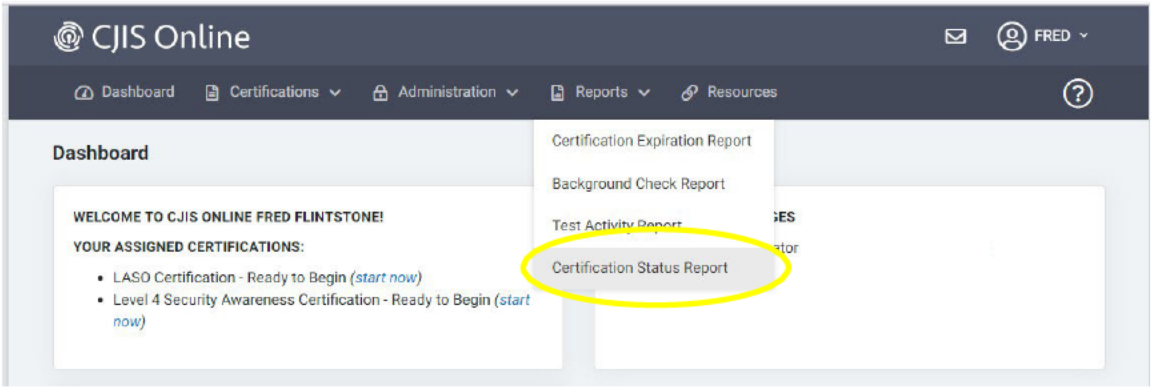


Sample of Certification Details tab.

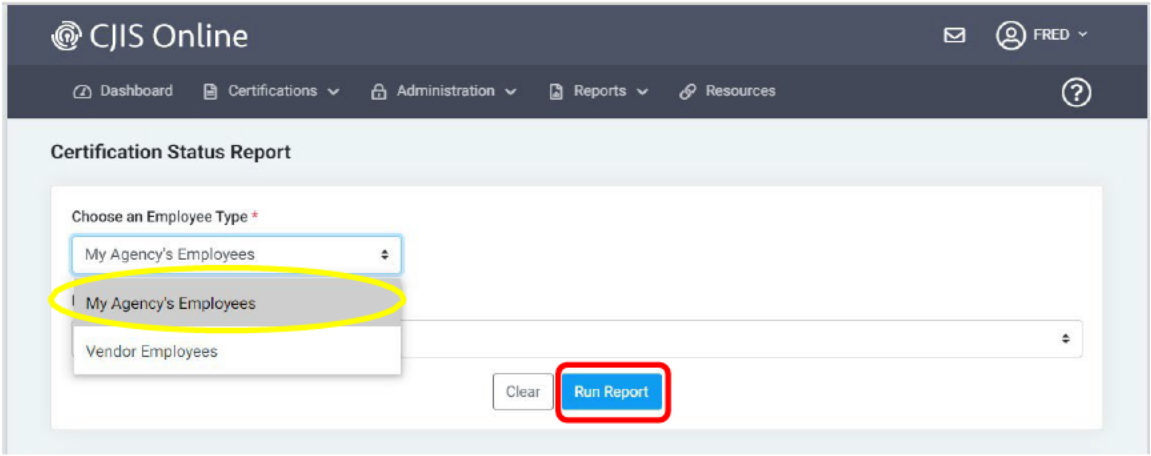
! Note: The *Background Checks* section on the Certification Details tab is **not** required to be filled in.

REPORTS

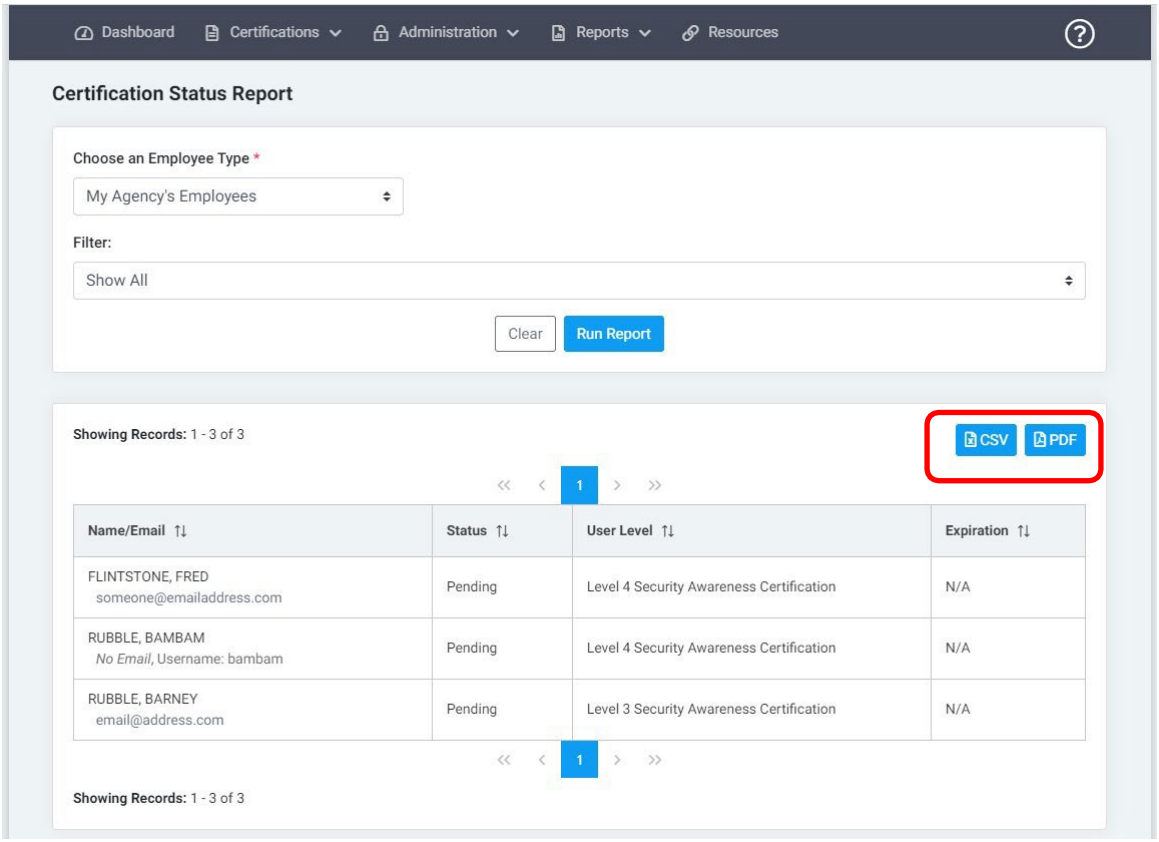
Click on **Reports.** Choose **Certification Status Report**.



To run a quick report of all employees.
Choose an Employee Type My *Agency's Employees.* Filter choose *Show All*
Click **Run Report.**

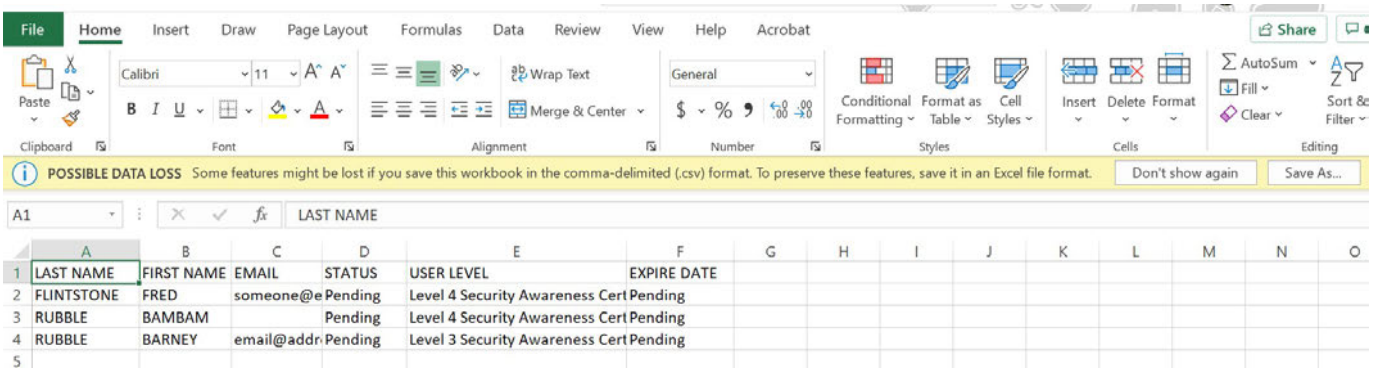


A viewable on-screen report appears.

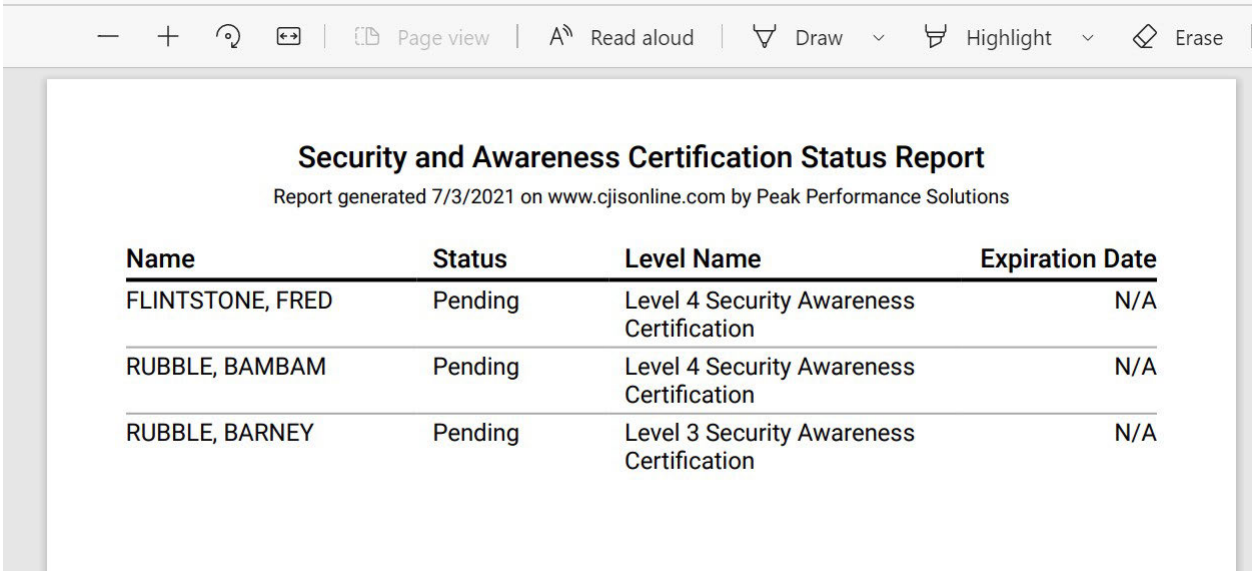


Sample of on-screen report.

To manange the records, the report can be made into an Excel sheet format for sorting the records or PDF version. Click on the **CSV** button for an Excel format or the **PDF** button for a read only PDF report.

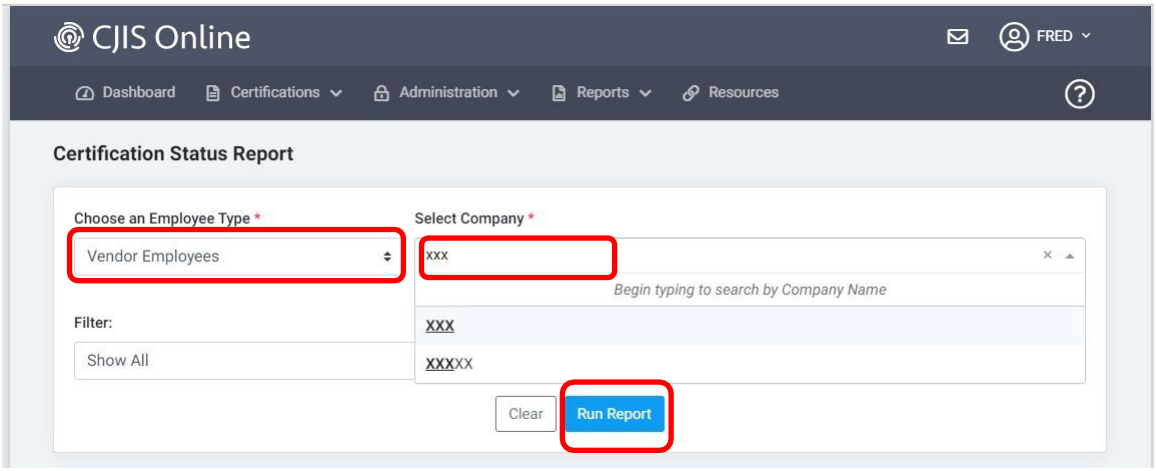


Sample of CSV Excel report. Save as an XLSX file on your computer.



Sample of a PDF report.

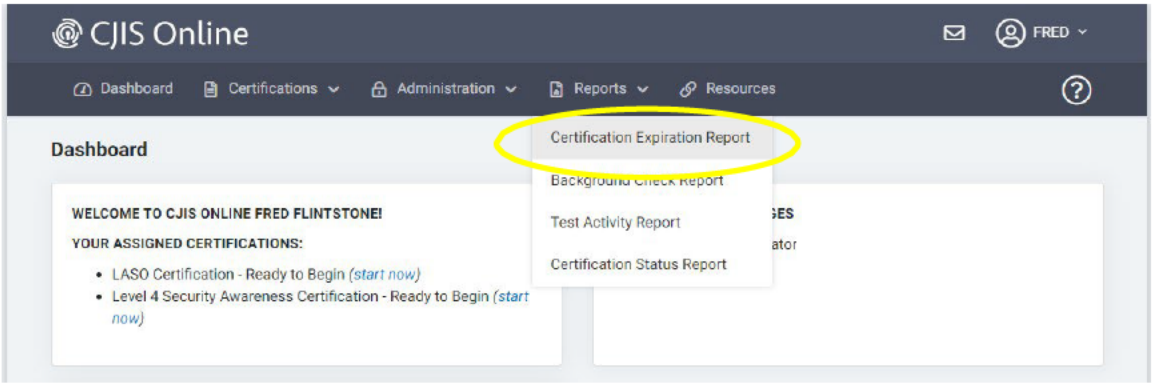
Similarly Vendor Reports can be run by choosing *Vendor Employees* from **Choose an Employee Type**
then start entering the company name in the **Select Company** box. After finding the company, **Run Report**.



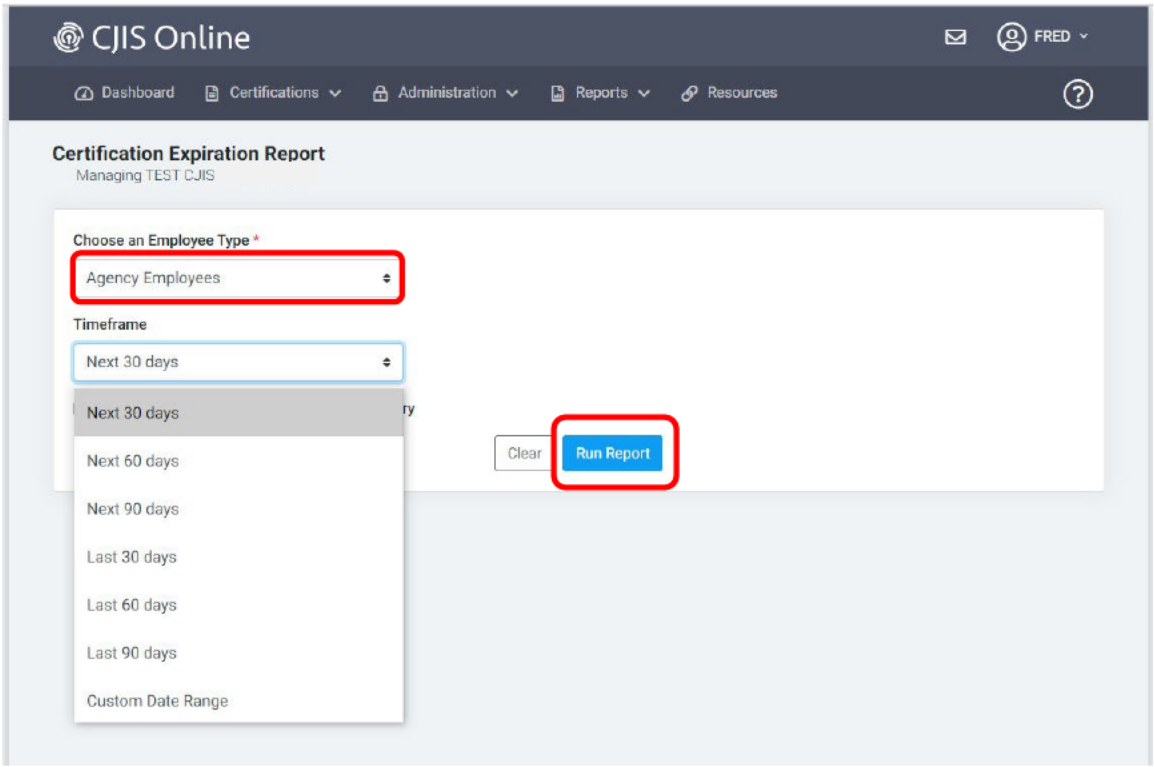
Sample of Vendor User Certification Status Report selection criteria on screen.

Run a Certification Expiration Report

Click on **Reports.** Choose **Certification Expiration report.**

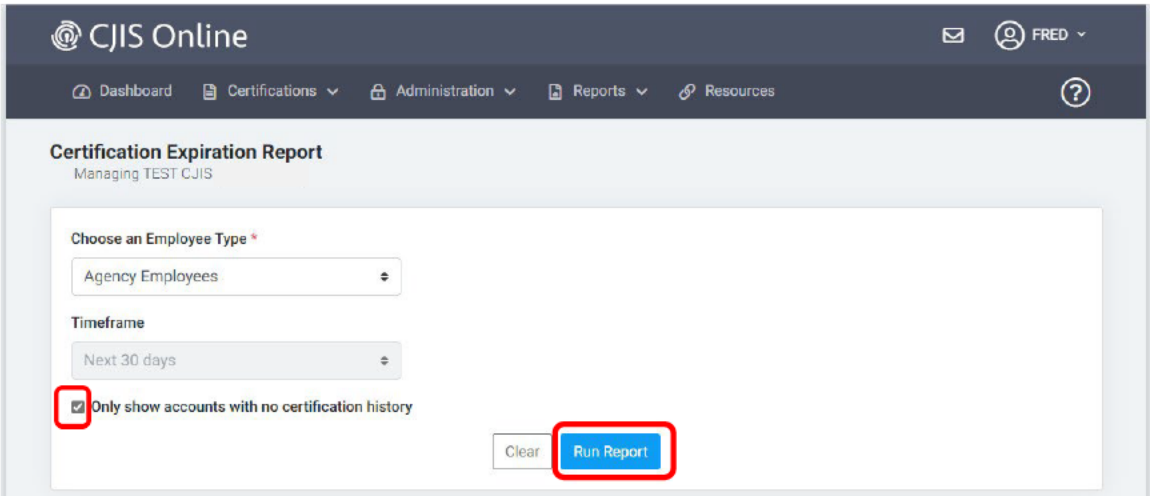


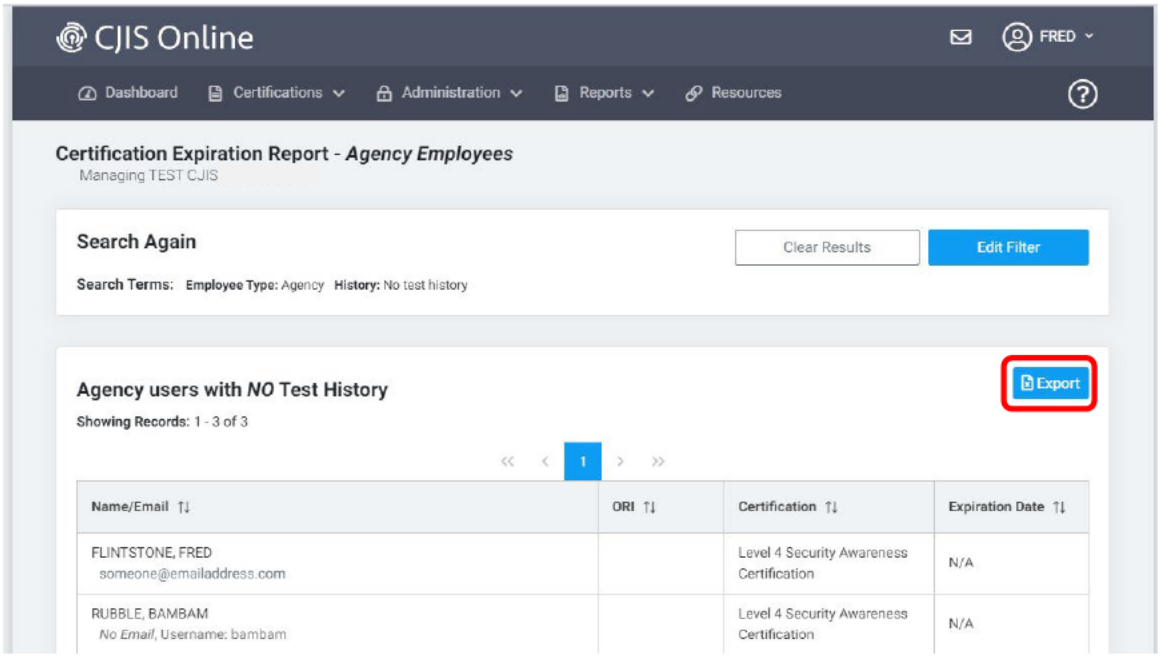
To run a report of all employee's certifications expiring; **Choose an Employee Type** *Agency Employees.*
Choose Timeframe from list or enter custom date range. Click **Run Report.**



To find accounts with no certification history.

On **Certification Expiration report** screen. Check off 'Only show accounts with no certification history.'
Run report.





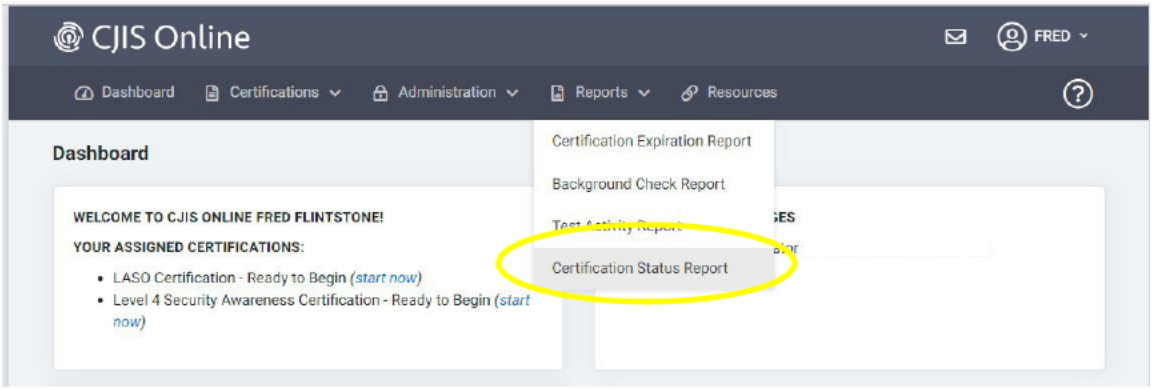
Sample of users with no test history report.

A result with N/A means there is no tests completed. Clicking the up/down arrows on the columnheadings allows the data to be sorted.

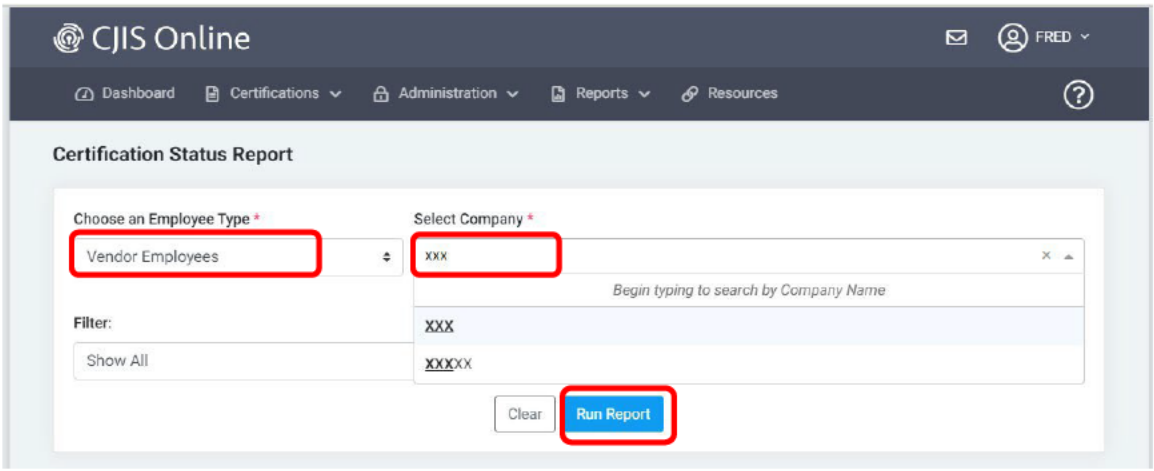
The **Export** button allows the data to be exported into an Excel Worksheet format. Click **Export** to put the data into an Excel sheet format. Remember to use File, Save As in Excel and save the worksheet on your computer.

To Run a vendor User Certification Expiration report

Click on **Reports.** Choose **Certification Expiration report.**



To run a quick report of a vendor's employees. Choose *Vendor Employees* from **Choose an Employee Type**
then start entering the company name in the **Select Company** box. After finding the company, **Run Report**.



! Good tip: If your vendor provides a list of personnel completing training, it is the agency's responsibility to check ifthe report is current and accurate.

A result with N/A means there is no tests completed. Clicking the up/down arrows on the column headings allow the data to be sorted. The reports are similar in appearance to the

agency’s user reports.

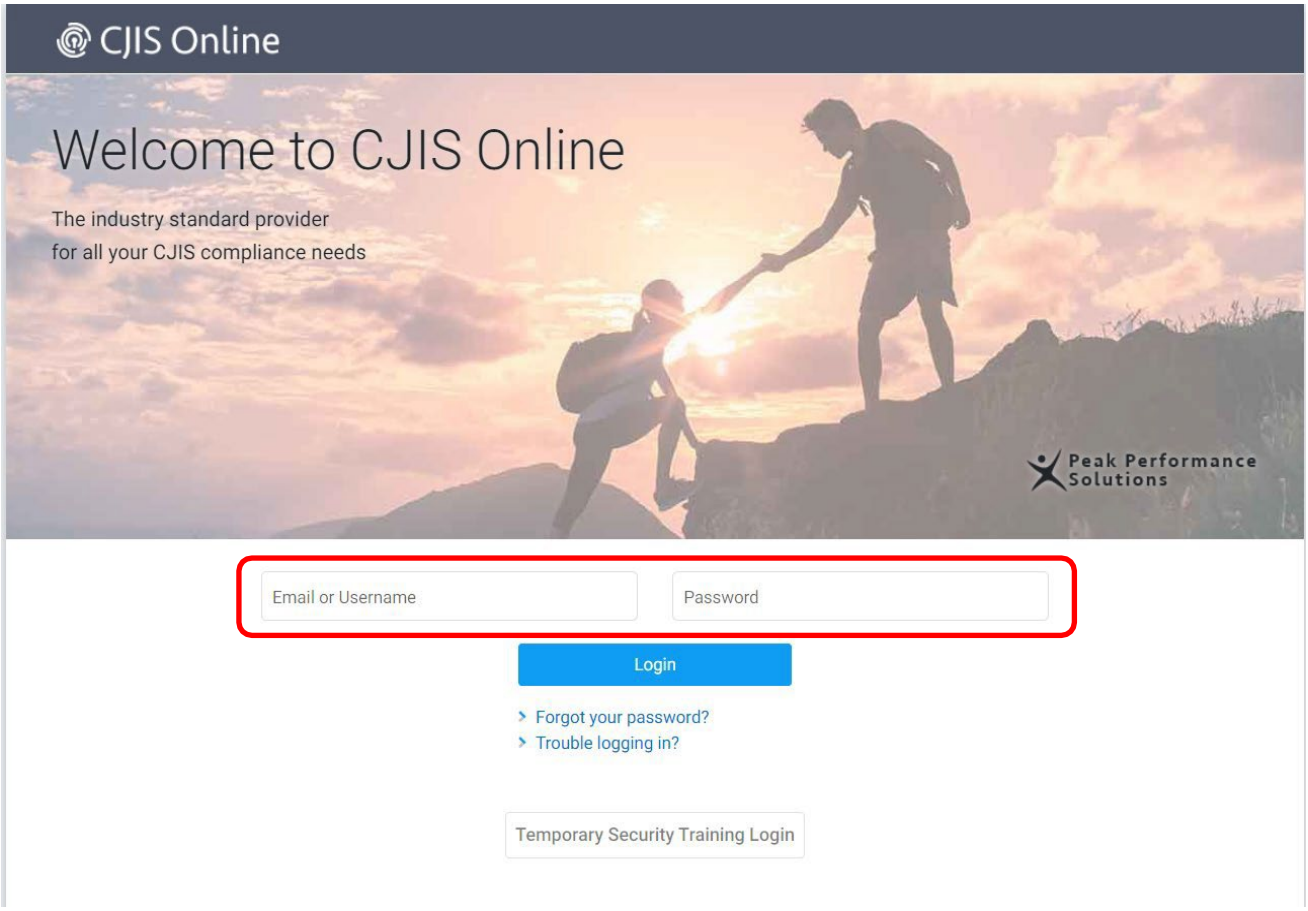
IT Staff & Agency User

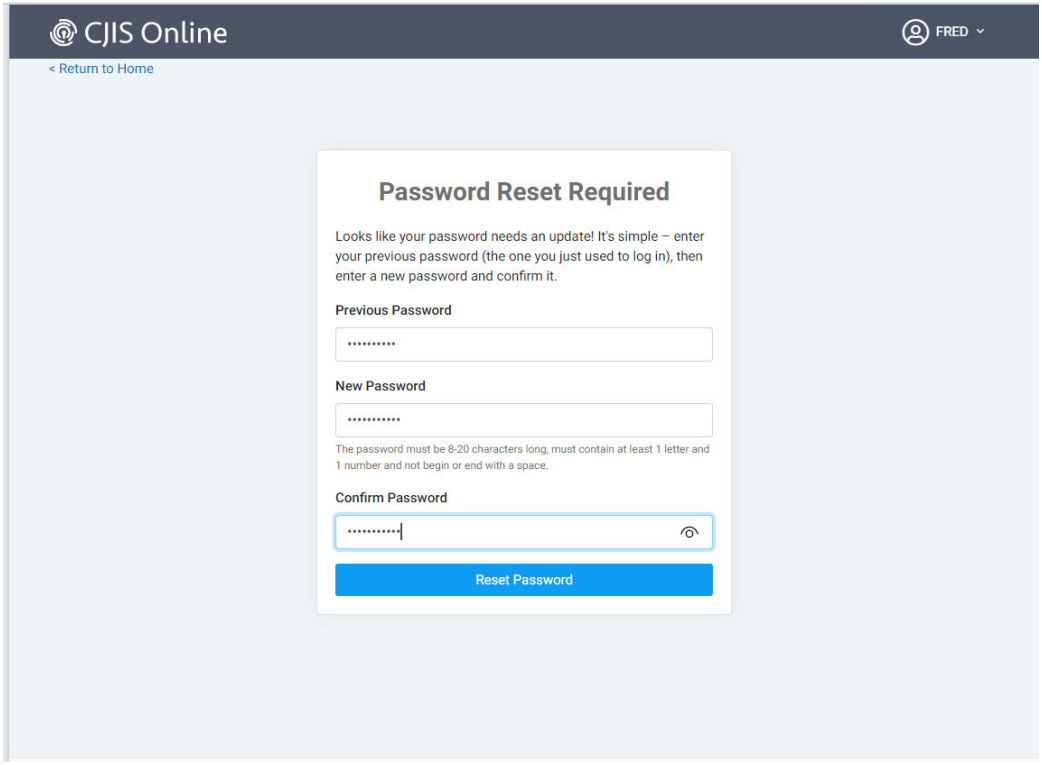
IT & Agency User Sign on

The individual will need their sign on information the agency Local Admin created to continue with training.

https://www.cjisonline.com

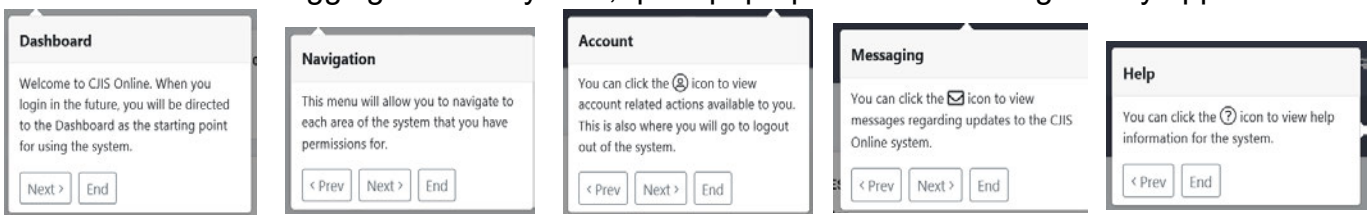
Enter the email / username and password. Click Login. Passwords are CaSe SeNsiTiVe.

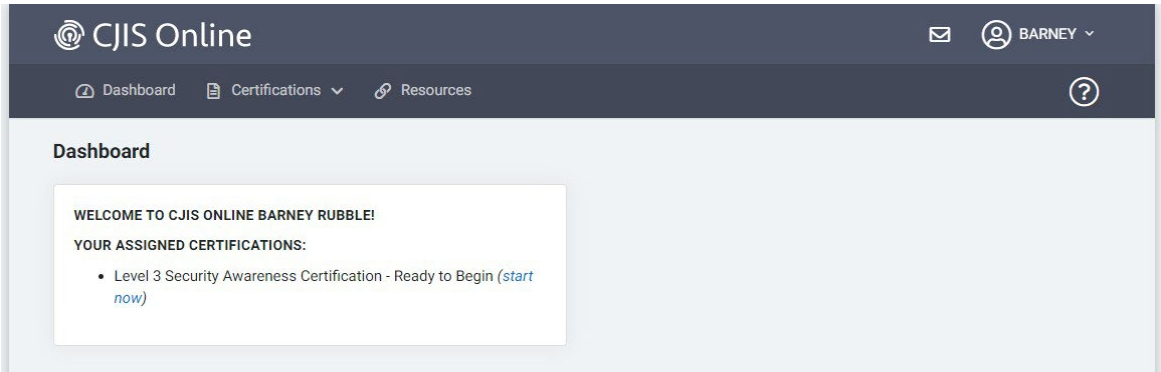




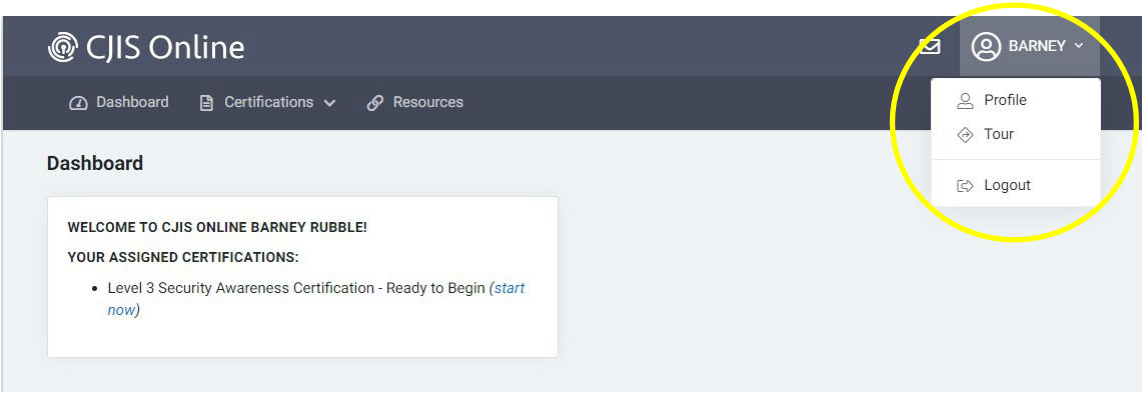
First time sign in, one may be prompted to change their password.
If needed, create a new password to continue. The fields are CaSe SeNsiTiVe.

First time logging into the system, quick pop-up notes or messages may appear.





This is the main Dashboard providing quick stats.



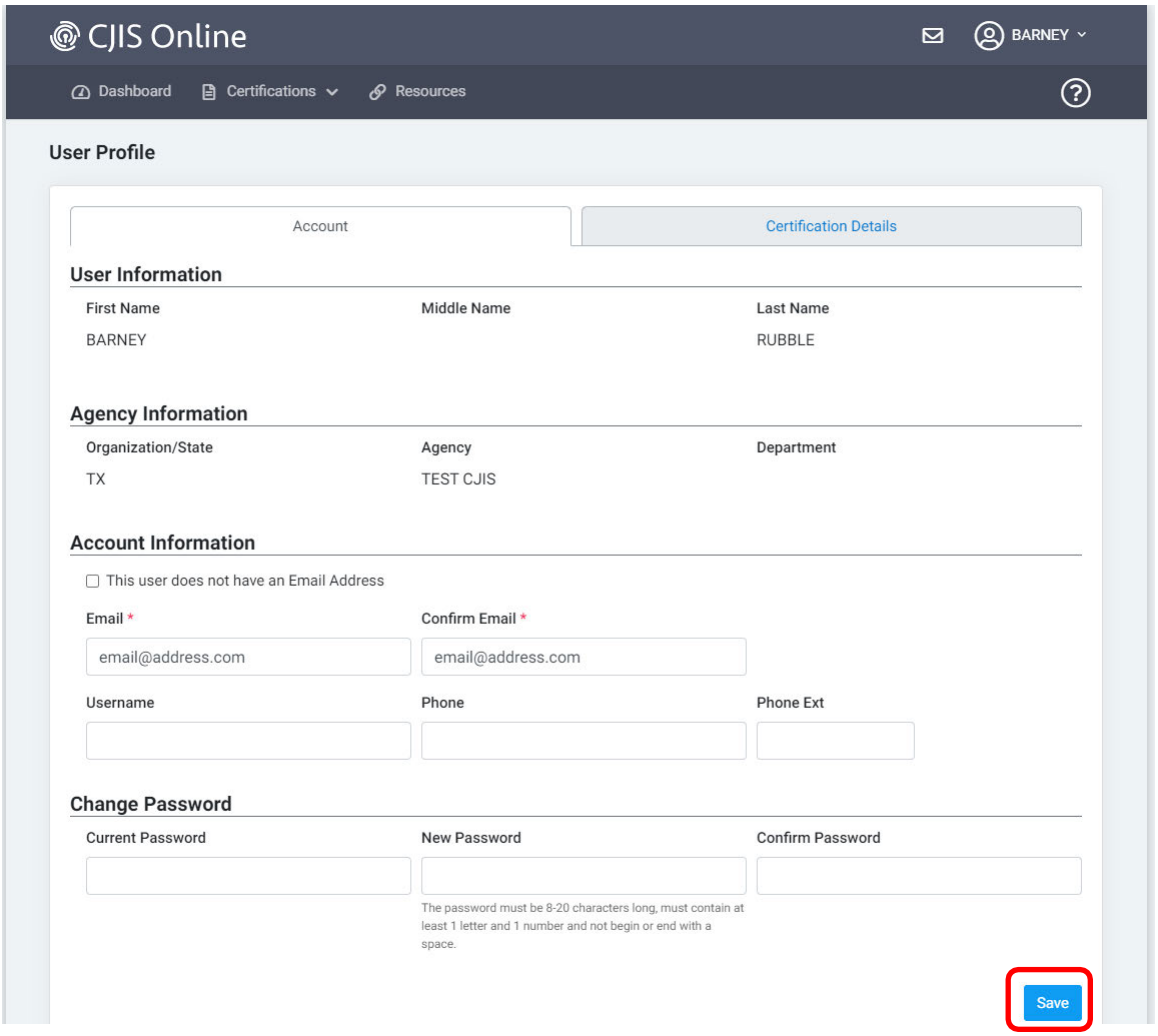
In the top right corner, click on the chevron symbol next to your name to view the Tour Notes again, **Edit** your Profile, view certificate details and certificate history, and use **Logout** to leave the system.

The **Envelope** contains messages from the application.



The task bar contains the main **Dashboard**, **Certifications** Menu, **Resources** Menu and **?** for additional help.

User Profile

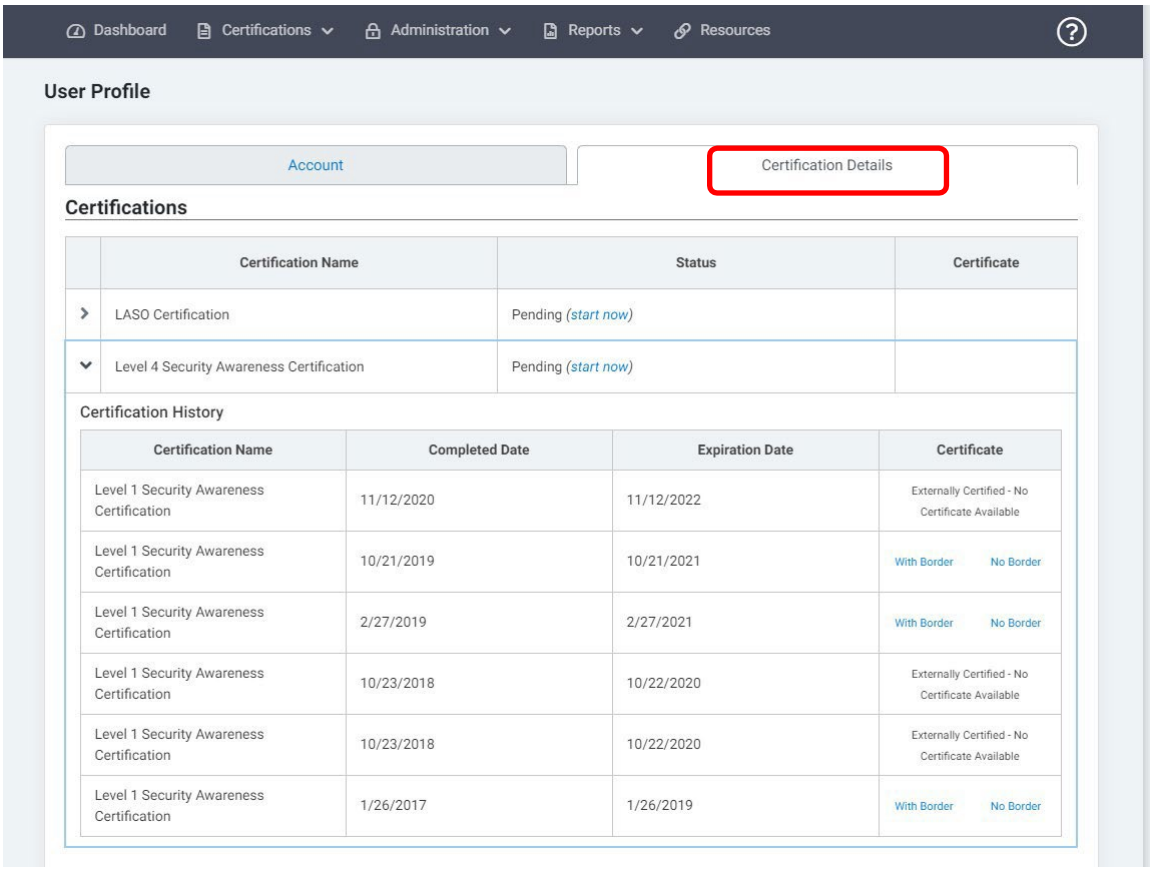


After clicking on **Profile,** the individual can only change account information pertaining to their account. Update email address, username, phone, and password then click **Save** when done.

Note: the account sign on is either the email address or username. Without a valid email address the userwill not be automatically notified to renew training.

Certification Details

Click on **Certification Details** tab.



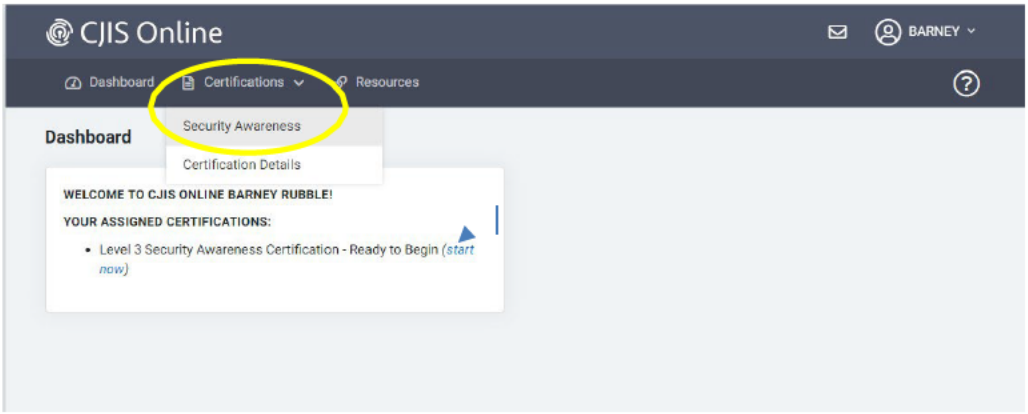
To view all the Certification history, click on the > greater than symbol, the symbol then points downward to open the history list. Find the available certificate in blue color, choose With Border or No Border.
Wait a few seconds for a screen to pop open with the certificate. After the screen opens, you may choose to print or save the certificate to your computer. If the certificate screen does not open, ensure pop-ups are not blocked by the browser and a supported Internet browser is being used.

The Local Agency Admin can also view and print certificates from their account.

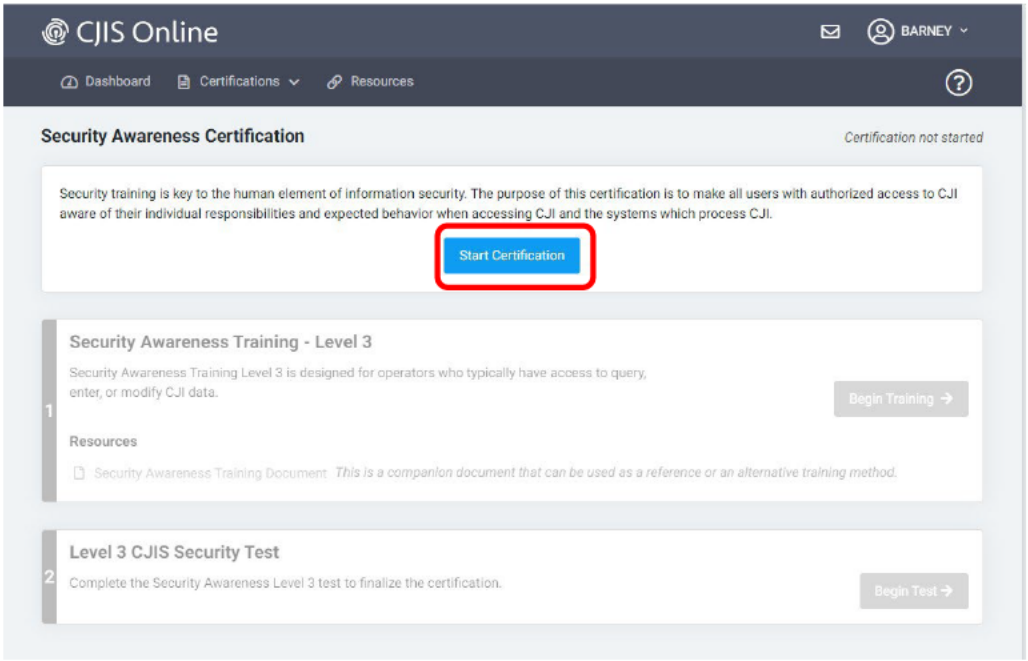
! Note: The *Background Checks* section on the Certification Details tab is **not** required to be filled in.

To Begin Training

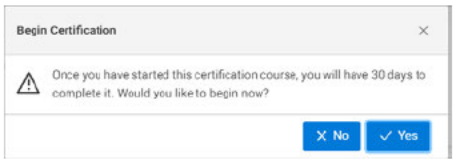
Click on **Certifications** then choose **Security Awareness**.

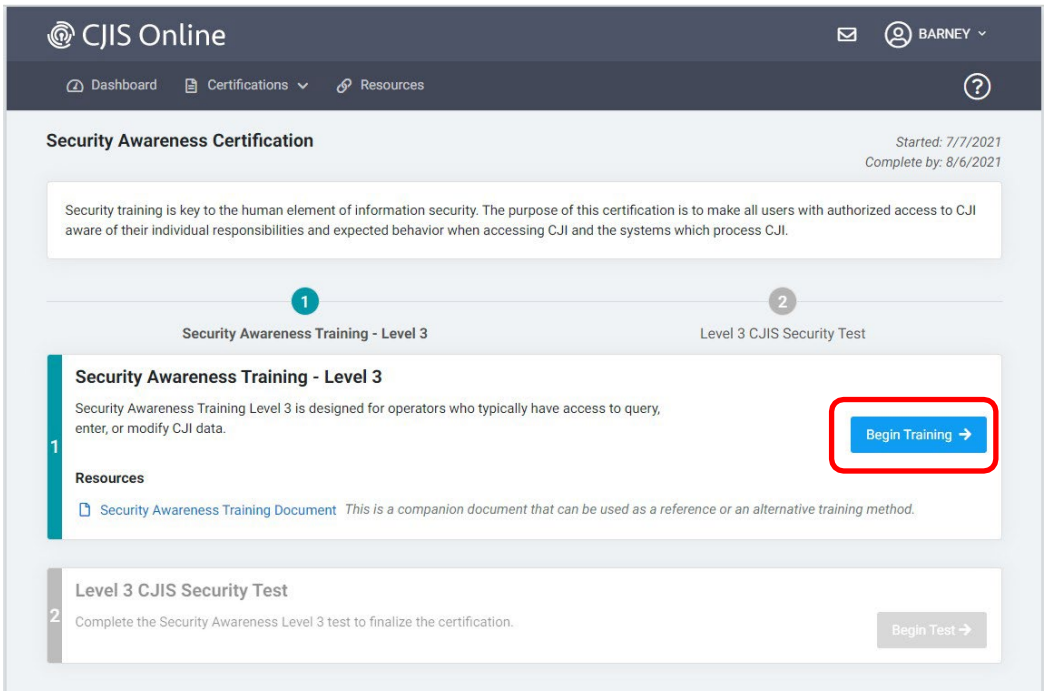


Alternate method: Click on the blue 'Start Now' on the main screen.

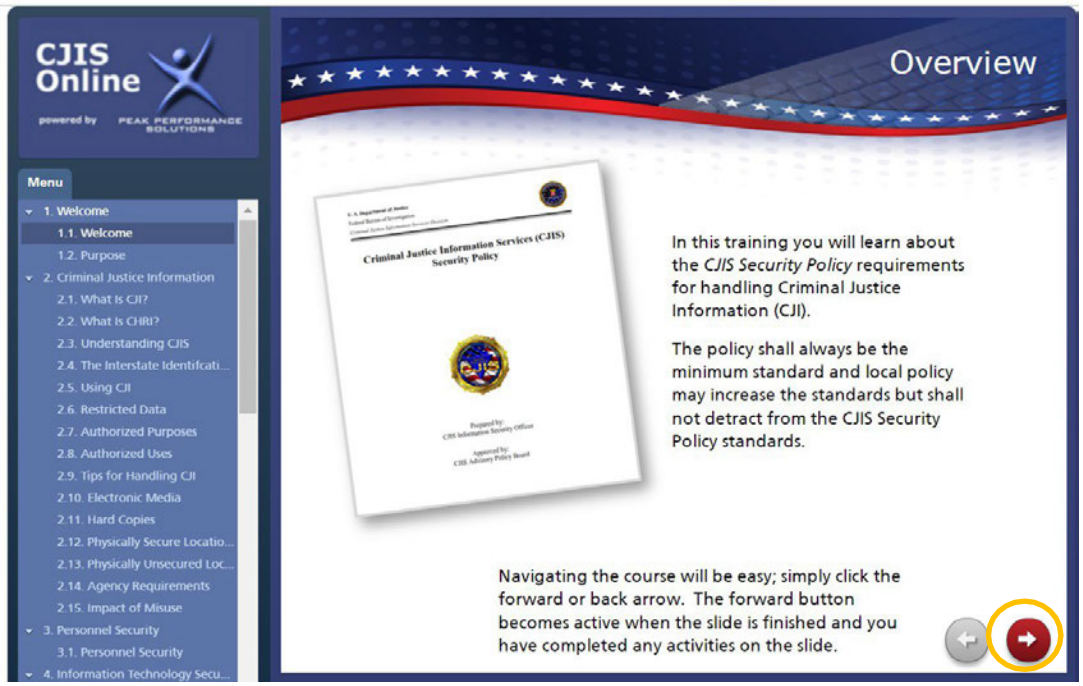


Click on the blue **Start Certification** button then confirm Yes or No.

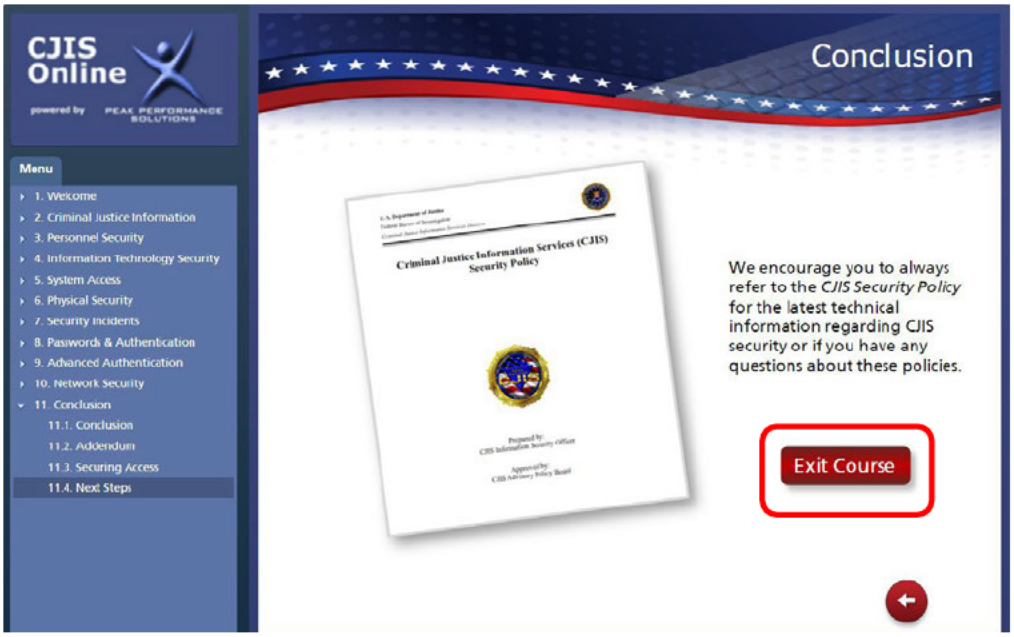




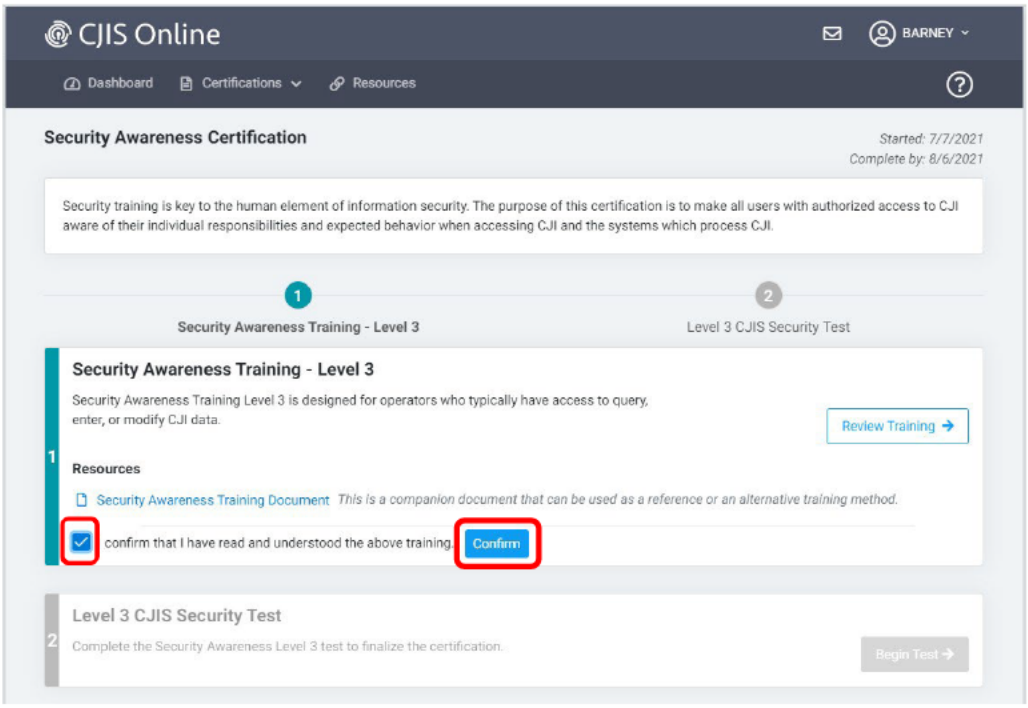
Click **Begin Training.**



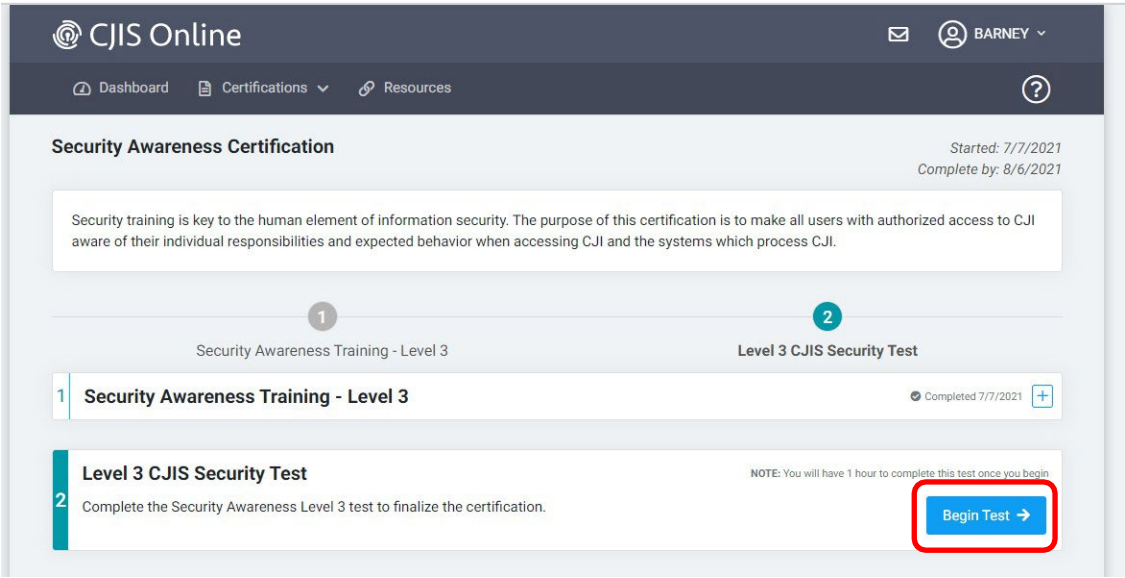
Read through the screens and click the arrows to get to the next screen.



Click **Exit Course** when done training and reviewing.



Check off the 'I Confirm…' box and then click on **Confirm** to continue.

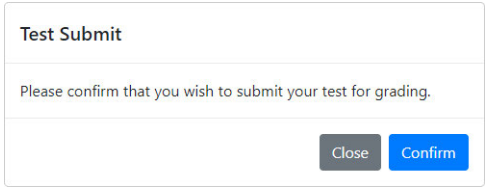


Click on **Begin**

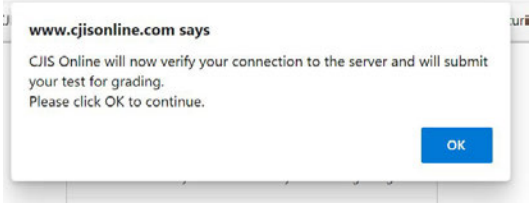
Test button. You will have 1 hour to

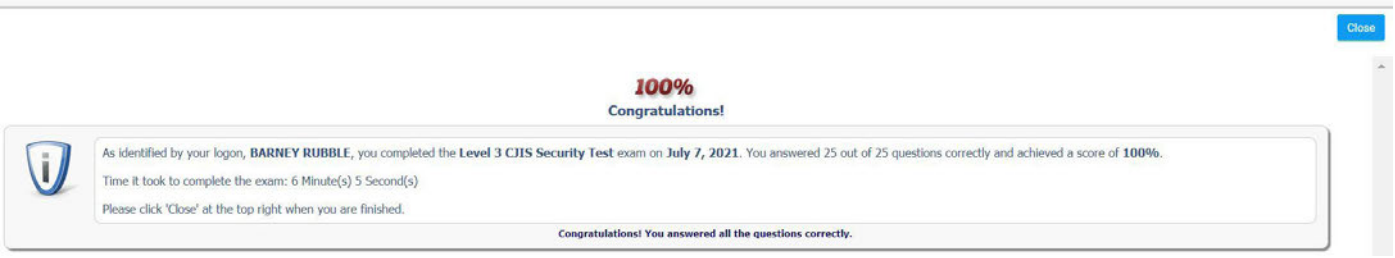
take the 25- question test.

To pass, you will need to achieve at least a 70 % (18 of 25 correct). After successful completion, this Certificate will be valid for two years.
If you do not pass, you will need to wait at least one hour before taking the test again. There are no limitations on how many times to retake the test.

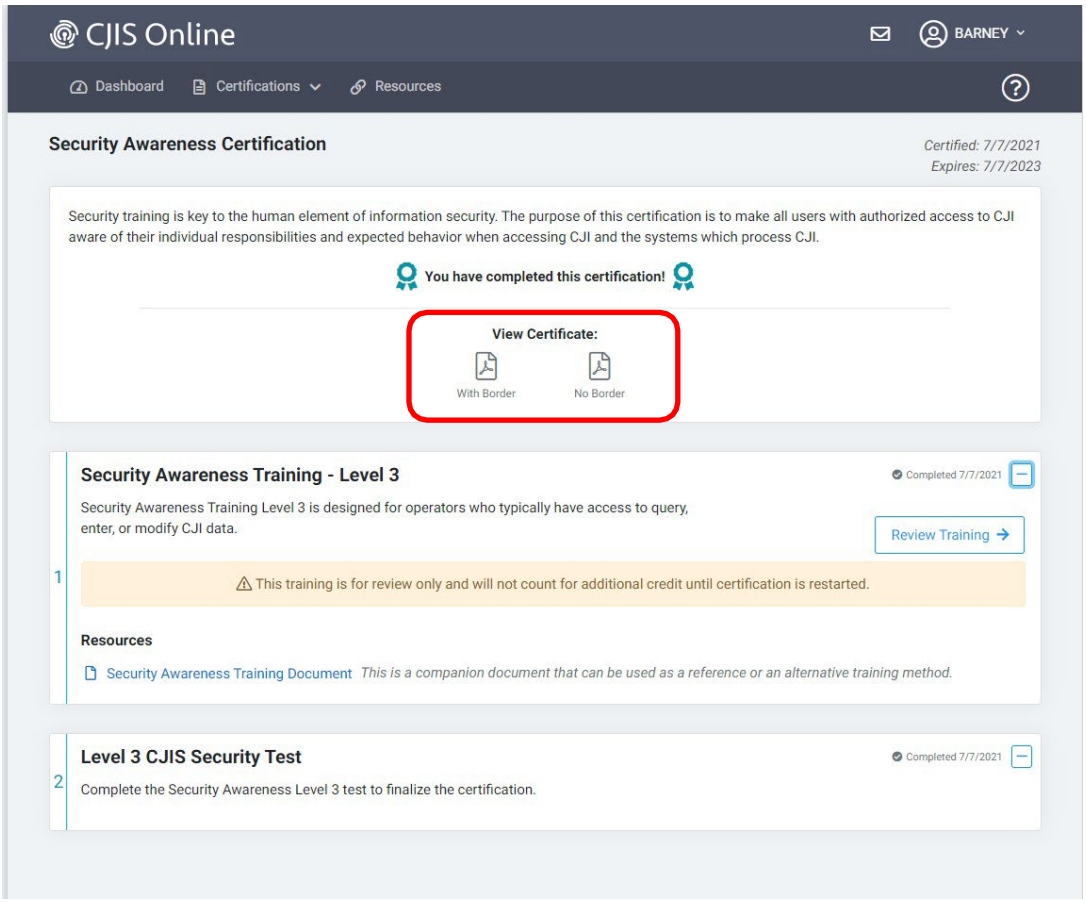


At the end of the test click **Confirm** button to submit test for grading then **OK** to message box below.



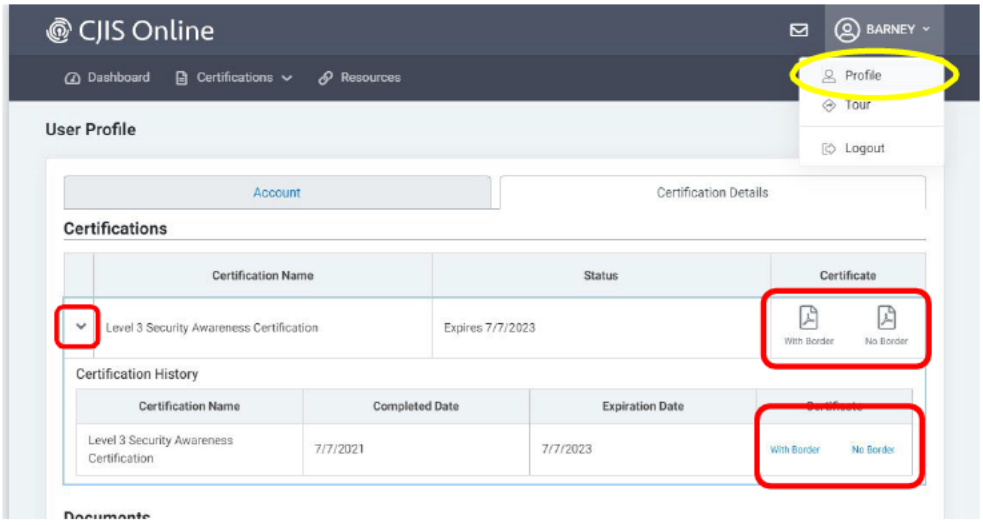


The test results appear and click **Close** button when done reviewing.



Once test successfully complete, you may print your certificate if desired. Under View Certificate section, click on With Border or No Border to view or print. Click on the printer or disk icon in top right corner to save or print certificate on next certificate screen.

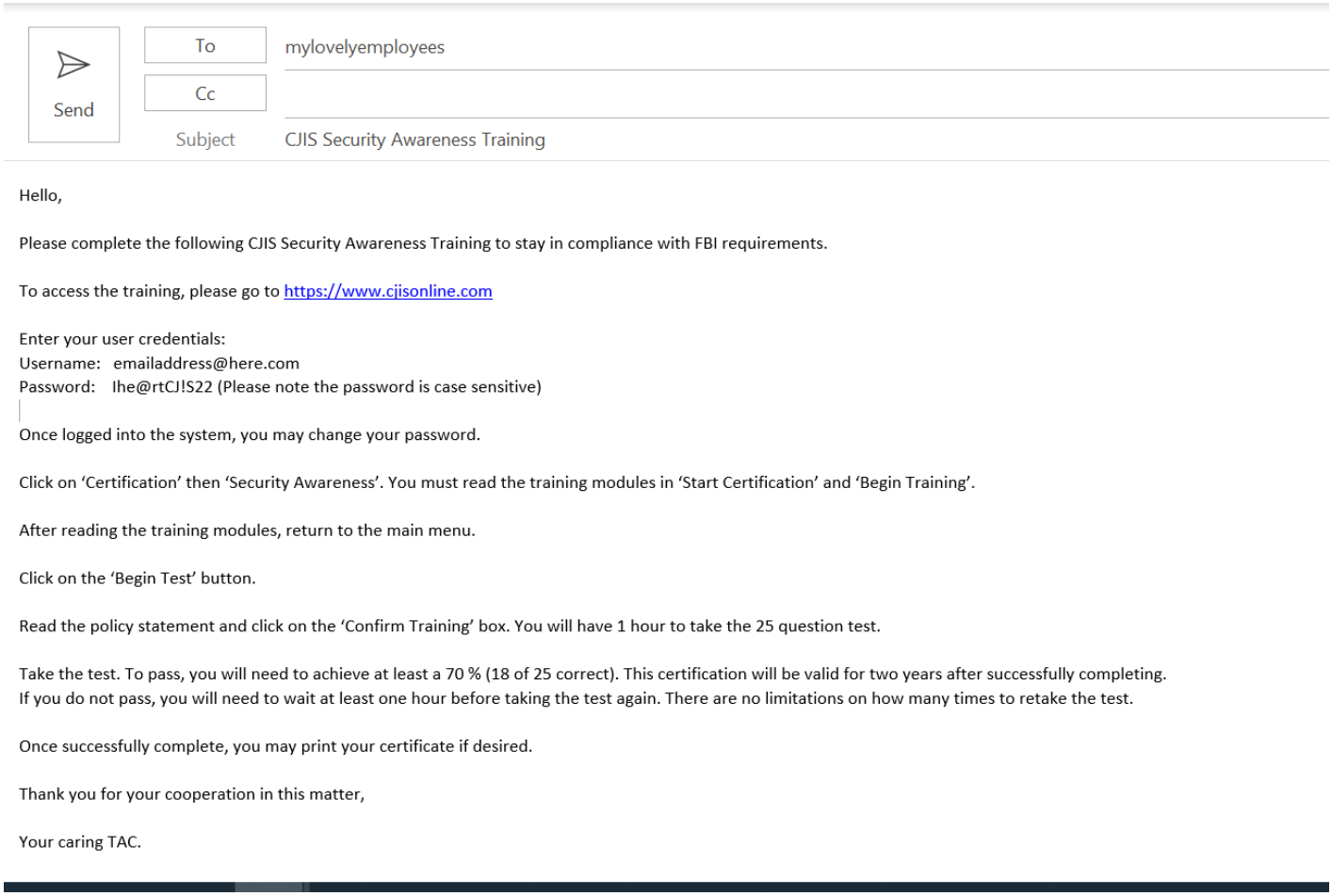




To print/reprint a certificate. In the top right corner, click on the chevron symbol next to your name, choose **Profile**, click Certificate Details tab. In the Certification history, click on the **>** greater
than symbol, the symbol then points downward to open the history list. Find the available certificate in blue color, choose With Border or No Border. Wait a few seconds for a screen to pop open with the certificate. After the screen opens,

you may choose to print or save the certificate to your computer. If the certificate screen does not open, ensure pop-ups are not blocked by the browser and a supported Internet browser is being used.

Email sample to send users for training



Send

To: mylovelyemployees

Cc:

Subject: CJIS Security Awareness Training

Hello,

Please complete the following CJIS Security Awareness Training to stay in compliance with FBI requirements.

To access the training, please go to https://www.cjisonline.com

Enter your user credentials:
Username: emailaddress@here.com
Password: Ihe@rtCJ!S22 (Please note the password is case sensitive)

Once logged into the system, you may change your password.

Click on 'Certification' then 'Security Awareness'. You must read the training modules in 'Start Certification' and 'Begin Training'.

After reading the training modules, return to the main menu.

Click on the 'Begin Test' button.

Read the policy statement and click on the 'Confirm Training' box. You will have 1 hour to take the 25 question test.

Take the test. To pass, you will need to achieve at least a 70 % (18 of 25 correct). This certification will be valid for two years after successfully completing.
If you do not pass, you will need to wait at least one hour before taking the test again. There are no limitations on how many times to retake the test.

Once successfully complete, you may print your certificate if desired.

Thank you for your cooperation in this matter,

Your caring TAC.

After creating a user account, you will need to provide the user an initial password and the link to get started. This is a sample of an email message to help with the planning.

Got questions, visit our web page for FAQs and other information to help.

APPENDIX C FORMS AND AGREEMENTS

MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES GLOBAL JUSTICE AND PUBLIC SAFETY USER AGREEMENT

1.0 Purpose

This Global Justice and Public Safety User Agreement (hereinafter, "Agreement") establishes guidelines for the access, use, dissemination, and sharing of criminal justice information (CJI) collected and maintained within the systems and networks operated, maintained, and managed by the Executive Office of Public Safety and Security (EOPSS) and/or the Massachusetts Department of Criminal Justice Information Services (DCJIS).

2.0 Authority

This Agreement is established pursuant to M.G.L. c. 6, § 167A, M.G.L. c. 6, § 18 ¾, 803 CMR 7.00, and 28 C.F.R. Part 20.

3.0 Parties and designees

The parties to this agreement include EOPSS, DCJIS and the criminal justice agency noted in the signatory section below. The parties collectively agree to follow the terms of said agreement. EOPSS designates DCJIS as its designee with the authority to audit and provide oversight of Public Safety Data Enterprise Applications within the scope of the Agreement. Furthermore, EOPSS also appoints DCJIS as it designee to sign this Agreement on behalf of both DCJIS and EOPSS.

4.0 Scope

This Agreement is applicable to all sworn and non-sworn employees, contractors, interns, volunteers, and information technology support staff of all criminal justice and public safety agencies in the Commonwealth of Massachusetts who utilize or otherwise have access to any Public Safety Data Enterprise Application, software application, system or network maintained, or managed by EOPSS and/or DCJIS.

Public Safety Data Enterprise Applications within the scope of this agreement include the following:

Automated License Plate Reader (ALPR) technology is a system that allows for the automatic recognition of license plates by a portable or stationary unit. The license plate information is then compared against a locally stored list of plates called the CJIS-NCIC Hotfile database which consists of license plate numbers associated with suspended or revoked licenses, stolen vehicles, AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Be On Look Out, and Wanted or Missing Person broadcasts where a license plate is included.

CopLink is a crime analytics platform application maintained by the Massachusetts State Police Fusion Center that allows for the inter-agency storage and sharing of various documents and information.

EOPSS Data Cross Tracking System is a data collection and reporting system for criminal justice agencies and the Trial Court, to

capture and report information on offenders and to report information relative to recidivism rates.

EOPSS National Incident Based Reporting System (NIBRS) Data Collection is a data collection and reporting system that criminal justice agencies submit incident and arrest data to in compliance with the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) standards.

My License Office (MLO) is an application that allows for the retrieval and use of Massachusetts' driver's license photos for various reasons, including professional licenses and identification cards.

The **Victim Notification Registry (VNR)** is the electronic application that allows for the registration of crime victims to receive notification of an offender's release from incarceration and certain CORI information.

This agreement may be amended from time to time to update the listing of Public Safety Data Enterprise Applications within the scope of this agreement.

5.0 Duration of Agreement

This Agreement is in effect until modified or cancelled by EOPSS and/or DCJIS. Each Agency Head shall sign off on a copy of this Agreement as a condition of access to the systems and networks operated, maintained, or managed by the EOPSS and/or DCJIS. In addition, each Agency Head will sign off on a copy of the Companion System Agreement for each system for which such an agreement exists. An original, signed copy of this Agreement, along with original, signed copies of any Companion System Agreements, will be kept on file at the DCJIS. The Agency Head shall maintain a copy of the signed agreements. Facsimile and electronic signatures are acceptable as originals.

The Agency Head also agrees to execute a new Global Justice and Public Safety User Agreement and all relevant Companion System Agreements in accordance with 803 CMR 7.06 whenever there are changes to the Agency Head, the CJIS Representative , the backup CJIS Representative, or the CJIS Technical Representative. The new Agreement(s) is/ are to be executed within ten (10) business days of the effective date of the change(s) necessitating a new Agreement(s). Original, signed copies of the newly executed Agreement(s) will be forwarded to the DCJIS within ten (10) days of execution.

6.0 Definitions

Authorized User
A sworn or non-sworn justice or public safety employee, contractor, intern, volunteer, or IT support staff member who has been authorized by his/her agency head to access any software application, system, network, or CJI operated, maintained, or managed by the DCJIS.

Companion System Agreement
An addendum or "rider" to this Agreement. Each Companion System Agreement establishes rules and protocols for contributing CJI to, or accessing, using, or disseminating CJI from, a specific system or database operated, maintained, or managed by the DCIJS.

Criminal Intelligence System
A system that stores detailed intelligence or investigative information on the suspected criminal activities of subjects and/or which stores only information designed to identify individuals or organizations that are the subject of an inquiry or analysis.

Criminal Justice Information (CJI)
CJI is defined as all data obtained from or through the CJIS or companion public safety data enterprise application necessary for law enforcement agencies to perform their missions. CJI includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Information System (CJIS) Representative
The CJIS Representative serves as the primary agency point of contact for the DCJIS. Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS- sponsored meetings, seminars, and conferences.

Criminal Justice Information System (CJIS) Backup Representative
The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. The Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Rep representative be unable to perform those duties and responsibilities for any reason.

Criminal Justice Information System (CJIS) Technical Representative
The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

Criminal Justice Information System (CJIS) User-Access Model
A single-identity management model used to authenticate users of the software applications, systems, and networks operated, maintained, or managed by the DCJIS.

Public Safety Data Enterprise Application
A software application which criminal justice and public safety agencies use to contribute CJI to, or to access CJI from, databases or systems maintained by or accessed through the DCJIS.

Non-Contributing Agency
An agency that may access CJI from, but which does not contribute CJI to, a database or system operated, maintained, or managed by the EOPSS or DCJIS.

Source Agency
The agency that originally recorded and contributed data to a database or system operated, maintained, or managed by EOPSS or DCJIS.

7.0 Transaction Logs

An audit log of all transactions made by CJIS user agencies is maintained by the DCJIS and EOPSS for systems maintained by EOPSS or DCJIS. This log records the identity of the individual user and agency accessing the system, the date and time of access, and the data entered into, or retrieved from, any database or system operated, maintained, or managed by the EOPSS or DCJIS. An Agency Head may request a report of all transactions initiated by the users of his/her agency. All report requests must be submitted in writing to the DCJIS.

The DCJIS CSO, at his/her discretion, may, at any time, authorize additional audits of all databases and systems operated, maintained, or managed by the EOPSS or DCJI S.

8.0 Audits of CJI Users

The DCJIS will conduct audits of all agencies, both criminal justice/public safety and non-criminal justice, accessing or using the CJI stored within, or obtained through, the databases, systems, and networks operated, maintained, or managed by the DCJIS. The purpose of these audits is to ensure the integrity and security of the CJI, applications, and systems, to investigate potential inappropriate use of these resources, and to identify potential training needs. Each CJIS user agencies will be audited at least on a triennial basis (once every 3 years).

9.0 Public Safety CJI, System, and Network Usage Restrictions

Use of any CJI obtained from or through an application, database, system, or network operated, maintained, or managed by the EOPSS or DCJIS is limited to authorized criminal justice purposes within the scope of a user's employment and official duties.

EOPSS and DCJIS resources may not be used for personal gain or for personal use, or to assist another individual or entity that is not authorized to access, use, or receive CJI from these resources. Criminal intelligence systems may also be subject to 28 CFR Part 23. Where the provisions of this Agreement or its addenda conflict with 28 CFR Part 23, 28 CFR Part 23 shall supersede this Agreement and its addenda.

10.0 Misuse

An Agency Head is responsible for investigating all alleged incidents or allegations of misuse of any CJI or database, system, or network operated, maintained, or managed by EOPSS or DCJIS. If an Agency Head determines that someone within his/ her agency has misused any of these resources, he/she must, within 10 business days, notify the DCJIS CSO in writing of the circumstances surrounding the misuse, of the actions taken, or to be taken, to address and correct the misuse, and of the policy(ies) and procedures to be implemented to prevent future misuse. The DCJIS CSO may suspend or revoke access to any or all databases or systems operated, maintained, or managed by the DCJIS for the individual(s) involved in the misuse.

Misuse of any EOPSS or DCJIS provided CJI or resource may result in individual loss of access to the resources, agency loss of access to the resources, and/or state

and federal civil and criminal penalties, if applicable. Users are also subject to the rules and regulations of their respective agency.

11.0 Access to EOPSS and DCJIS Resources

Sworn and non-sworn justice and public safety employees, as well as the employees of non-criminal justice agencies, may be granted access to one or more DCJIS applications, systems, and networks as authorized by the Agency head.

Each individual accessing an EOPSS or DCJIS resource will be assigned a unique user identifier (User ID) and initial password. The individual will be required to change his/her password when logging into a resource for the first time. When possible, the same User ID and Password will enable a user to access multiple EOPSS and DCJIS resources. However, some applications may require a separate log in and/or a different User ID and Password.

All passwords used to access an EOPSS or DCJIS resource will meet the DCJIS and FBI security requirements in effect at the time the password is created/changed.

Authorized users shall not share their passwords and user identifications with any other individual. Each authorized user shall be responsible for all transactions conducted with his or her user identification and password.

Agencies are responsible for notifying the EOPSS or DCJIS, in writing, when a user is no longer authorized to access and EOPS or DCJIS resource. EOPSS or DCJIS will terminate or suspend user access depending on the user's status within his/her respective agency.

User IDs and passwords shall be reviewed by each agency on an annual basis. The Agency Head and agency CJIS Representative shall be responsible for this review. The purpose of this review is to confirm the continued authorization of all individuals accessing DCJIS resources. The Agency Head and CJIS Representative shall annually certify the accuracy of his/her agency's authorized user list to the DCJIS CSO.

12.0 Ownership of CJI Contained Within EOPSS or DCJIS Databases and Systems

The Source Agency will maintain ownership of, and responsibility for, the CJI it enters or modifies within any database or system operated, maintained, or managed by the EOPSS or DCJIS.

The Source Agency will exercise due diligence to ensure that the CJI it enters is current, complete, and accurate. Each Source Agency is also responsible for ensuring that the CJI it contributes is in compliance with all federal, state, and local laws.

User agencies shall communicate any errors found in CJI contained in any database or system operated, maintained, or managed by the DCJIS to the Source agency for that CJI as well as to the EOPSS or DCJIS.

13.0 Dissemination of CJI

CJI contained within, or obtained through, any database, system, or network operated, maintained, or managed by the EOPSS or DCJIS shall only be disseminated to other authorized agencies and individuals. In addition, the CJI obtained within, or obtained through, any DCJIS resource shall only be used for authorized criminal justice purposes.

14.0 Public Records

Records maintained within the databases and systems operated, maintained, or managed by the EOPSS or DCJIS are subject to the Massachusetts Public Records Law as defined in M.G.L. c. 4, s. 7(26).

All responses to public record requests for information contained in an EOPSS or DCJIS resource shall be referred to the Agency that contributed the relevant information for its response as the custodian of the record(s).

The EOPSS or DCJIS CSO may respond to a public records request for statistical data drawn from an EOPSS or DCJIS resource.

15.0 Data Submission and Retention Policy

Source Agencies shall contribute data to each EOPSS or DCJIS database or system pursuant to the schedule established in the Companion System Agreement for that database or system, if applicable. Companion System Agreements are attached to this Agreement as Addenda.

Data maintained in an EOPSS or DCJIS database(s) and system(s) shall be retained pursuant to the schedule established in the Companion System Agreement for that respective system, if applicable.

16.0 Data Submission Standards

For each system that requires the contribution of data by Source Agencies, those Agencies shall submit at least the minimum set of data as established in the guidelines or any Companion System Agreement if required, for the respective subject application.

17.0 Designation of an Agency Representatives

CJIS Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the EOPSS or DCJIS shall appoint a CJIS Representative. The CJIS Representative serves as the primary agency point of contact for the EOPSS and DCJIS. Responsibilities include ensuring that all EOPSS and DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the EOPSS or DCJIS or who use the CJI obtained from or through those systems and networks, and attending all EOPSS or DCJIS- sponsored meetings, trainings, seminars, and conferences.

Backup CJIS Representative*:*
Each agency that accesses or uses CJI obtained from or through the systems or networks operated, maintained, or managed by the DCJIS shall also appoint a Backup CJIS Representative. The Backup CJIS Representative shall be the EOPSS

and DCJIS' secondary point of contact for the agency. In addition, the Backup CJIS Representative shall assume all the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

CJIS Technical Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Technical Representative. The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

18.0 Technical Support

The Executive Office of Public Safety and Security (EOPSS) Office of Technology and Information Services (OTIS) shall provide technical support services for all applications, databases, systems, and networks, operated, maintained, or managed by the EOPSS or DCJIS.

19.0 Internal Agency Policies

Each agency obtaining CJI either directly from, or through, an application, database, system, or network operated, maintained, or managed by the EOPSS or DCJIS shall draft and adopt internal policies to inform and ensure that agency authorized users have read and agree to comply with the provisions of this Agreement and its Addenda.

20.0 Termination of Access

An agency may request termination of its access to one or more EOPSS or DCJIS resources by providing a written request to the DCJIS CSO.
The DCJIS CSO may also terminate access to a DCJIS resource pursuant to the terms of a Companion System Agreement.

21.0 Amendments

Any change in the provisions of this Agreement or in the provisions of a Companion System Agreement shall be incorporated by a written amendment approved by the EOPSS and DCJIS CSO.

22.0 Global Justice and Public Safety User Agreement Signoff

By signing this Agreement, the Agency Head acknowledges he/ she has read and understood its provisions and that he/she will comply with its terms and conditions.

_____ _____ Agency Head Name/Title	Commissioner, Department of Criminal Justice Information Services
_____ Agency	
_____ _____ Agency Head Signature	DCJIS Commissioner Signature
_____ _____ Date	Date

MEMORANDUM OF UNDERSTANDING CRIMINAL JUSTICE AGENCYMOBILE DATA SHARING HOST/USER GUIDELINES

Once executed by all parties, this MOU must remain on file with the Host, the User, and the Department of Criminal Justice Information Services (DCJIS).

This Memorandum of Understanding (MOU) is entered into this _____day of_____, 20_____ by and between _____, a criminal justice agency hereafter referred to as the **Host,** and _____, a criminal justice agency hereafter referred to as the **User**.

This MOU is intended to define the terms, conditions, and mutual responsibilities of the parties hereto, for the purpose of enabling the User access, via the User's mobile data terminals, to the Massachusetts Criminal Justice Information System (CJIS), including access to Registry of Motor Vehicle (RMV) data and images, to FBI CJIS systems, including the National Crime Information Center (NCIC), and to the International Justice and Public Safety Network (Nlets), utilizing the Host's server, the Host's CJIS router, and other hardware and software necessary to operate wireless devices. This MOU incorporates by reference, and operates in conjunction with, the Massachusetts CJIS User Agreement and the FBI CJIS Security Policy. Both parties agree to adhere to all Massachusetts CJIS policies and to the policies of both the FBI and Nlets.

The User and Host agree:

a. To be bound by the conditions of this MOU and to notify each other and the DCJIS in the event that any of the conditions stated in this Agreement change in the future.
b. To execute this MOU with the DCJIS biennially as long as the Host/User relationship continues.
c. To notify the DCJIS of pending relationship termination immediately, as provided in the final paragraph of this MOU.
d. To develop and maintain a separate written agreement which includes procedures that clearly identifies the responsibilities of each agency when a mobile/wireless server is not functioning, and which department is responsible for managing the vendor response process. This agreement must detail the maintenance process and identify (1) who is responsible for contacting the DCJIS for service issues and (2) who is responsible for costs associated with the server and usage.
e. **That calls for service to the DCJIS must be made by the Host Agency;** and
f. That a violation of this MOU shall be considered a violation of the CJIS User Agreement between the violating party and the DCJIS.

The Host understands that the use of the Host's server by another criminal justice agency is not standard protocol and that the DCJIS only agrees to this arrangement where such access is necessary to aid the User criminal justice agency in the performance of the User's official criminal justice duties. The Host hereby agrees to:

a. Allow the User to utilize the Host's base system for access to any and all available information on the CJIS, RMV, FBI, and Nlets systems, via approved wireless devices, provided that the dissemination of such information would not be a violation of any laws or regulations of the United States or of the Commonwealth of Massachusetts.
b. Provide assistance in the furtherance of criminal justice information (CJI) processing and communications through record inquiry, message transmittals, or record entries

in keeping with all standards, and further agrees to limit access to such information to authorized employees of the User; and

c. Maintain an automated log of inquiries or transactions made by any of the User's wireless devices. The log must include the identification of the specific wireless device from which the inquiry was made, the operator of the device, the operator's department, and the date and time of the inquiry or transaction. Each log entry must be maintained by the Host for a minimum of one year and must be provided to the DCJIS and to the FBI upon request.

The User hereby acknowledges that it understands, and shall advise all its employees of, the penalties relating to unauthorized access to, or dissemination of CJI as defined in the Criminal Offender Record Information (CORI) Act (M.G.L. c. 6, § 167 et seq.), in 803 C.M.R. 2.00-9.00 et seq., in 28 CFR, in the CJIS User Agreement, and in the FBI CJIS Security Policy. The User agrees:

a. To abide by all laws of the United States and the Commonwealth of Massachusetts, as well as by the rules and regulations of the responsible administrative agencies, including the DCJIS as the FBI CJIS Systems Agency (CSA), and the FBI.
b. To abide by the standards and conditions of the CJIS User Agreement concerning the security, entry, collection, storage, verification, retrieval, access, and dissemination of CJI.
c. That the Host's system will be used for inquiries only; and
d. That all its personnel with access to wireless devices that will utilize the Host's base system have been trained, tested, and certified as required by the DCJIS and the FBI.

Either the Host or the User may, upon thirty days written notice to the other party and to the DCJIS, cancel this MOU in its entirety. Upon determination that the User has violated the terms of this MOU, the Host, in cooperation with the DCJIS, reserves the right to terminate this MOU with or without notice. The DCJIS may terminate this MOU at any time and without notice.

In witness thereof, the above-named parties have signed this document in full agreement on this _____day of_____, 20___.

USER AGENCY: _____ **HOST AGENCY: _____**

By: _____ By: _____

(Signature of Chief/Agency Head) (Signature of Chief/Agency Head)

Title: _____ Title: _____

Date: _____ Date: _____

CJIS Systems Officer: _____ Date: _____

Jamison R. Gagnon

MEMORANDUM OF UNDERSTANDINGUSE OF A CRIMINAL JUSTICE AGENCY CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS) ROUTER and SWITCH BY A NON-CRIMINAL JUSTICE AGENCY

Once executed by all parties, this MOU must remain on file with the Host, the User, and the DCJIS.

This Memorandum of Understanding (MOU) is entered into this _____day of_____, 20___ by and between _____, a criminal justice agency, hereafter referred to as the **Host,** and _____, a non-criminal justice agency, hereafter referred to as the **User**.

This MOU defines the terms, conditions, and mutual responsibilities of the parties hereto, for the purpose of enabling the User to access the Host's/User's internal Computer-Aided Dispatch (CAD) system and/or Records Management System (RMS) via mobile data terminals utilizing the Host's CJIS router and switch. This MOU incorporates by reference, and operates in conjunction with, the standard Massachusetts CJIS User Agreement, which includes agreement by the Host to adhere to the Federal Bureau of Investigation's (FBI's) Criminal Justice Information System (CJIS) Security Policy (hereinafter, the CSP). It is the Host's responsibility to ensure that its CJIS User Agreement with the DCJIS is current and on file at the DCJIS Support Services Unit and with its Agency Head.

The User and Host agree:

a. To be bound by the conditions of this MOU and to notify each other and the DCJIS in the event that any of the conditions stated in this Agreement change in the future;
b. To execute a new MOU with the DCJIS once every two (2) years as long as the Host/User relationship continues;
c. To notify the DCJIS of pending termination immediately, as provided in the final paragraph of this MOU;
d. To develop and maintain a written agreement that includes a procedural statement that clearly identifies the responsibilities of each agency;
e. **That calls for service to the DCJIS must be made by the Host criminal justice agency;**
f. That a violation of this MOU shall be considered a violation of the CJIS User Agreement between the violating party(ies) and the DCJIS.

The Host understands that the use of the CJIS router and switch by a non-criminal justice agency is not standard protocol and that the DCJIS only agrees to this arrangement where such access is necessary to aid the User non-criminal justice agency in the performance of its official public safety duties.

The Host hereby agrees to only allow the User to utilize the CJIS router and switch to access User data systems in the performance of its public safety duties. Access to any CJIS or Criminal Offender Record Information (CORI) data systems is prohibited.

The Host hereby acknowledges an understanding of, and shall advise all its employees and user agency personnel of, the penalties relating to illegal actions with regard to criminal justice information, the Criminal Offender Record Information (CORI) Act as found in M.G.L. c. 6, § 167 et seq., the CJIS User Agreement, and the CSP.

The User agrees that the Host's CJIS router and switch will be used to access non-CJIS and/or non-CORI data only, which will aid in the performance of its official public safety duties, provided that the dissemination of such information would not be a violation of any laws or regulations of the United States or of the Commonwealth of Massachusetts.

Either the Host or the User may, upon thirty (30) days notice to the other party and to the DCJIS, in writing, cancel this MOU in its entirety. Upon determination that the Host or User has violated any law, rule, or regulation concerning criminal justice information or the use of the Host's CJIS router and/or switch, or violated the terms of this MOU, the Host or User, in cooperation with the DCJIS, reserves the right to terminate this MOU with or without notice. The DCJIS may terminate this MOU at any time and without notice.

USER: _____ **HOST:** _____

***By:** _____ ***By:** _____

Title: _____ Title: _____

Date: _____ Date:_____

Print Name: _____ Print Name: _____

DCJIS:

*By: _____

Title: _____Commissioner_____

Date: _____

Print Name: ___Jamison Gagnon_____

***Signature of person who is legally authorized to sign for the agency.**

MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES
GLOBAL JUSTICE AND PUBLIC SAFETY USER AGREEMENT

2.0 Purpose

This Global Justice and Public Safety User Agreement (hereinafter, "Agreement") establishes guidelines for the access, use, dissemination, and sharing of criminal justice information (CJI) collected and maintained within the systems and networks operated, maintained, and managed by the Executive Office of Public Safety and Security (EOPSS) and/or the Massachusetts Department of Criminal Justice Information Services (DCJIS).

2.0 Authority

This Agreement is established pursuant to M.G.L. c. 6, § 167A, M.G.L. c. 6, § 18 ¾, 803 CMR 7.00, and 28 C.F.R. Part 20.

4.0 Parties and designees

The parties to this agreement include EOPSS, DCJIS and the criminal justice agency noted in the signatory section below. The parties collectively agree to follow the terms of said agreement. EOPSS designates DCJIS as its designee with the authority to audit and provide oversight of Public Safety Data Enterprise Applications within the scope of the Agreement. Furthermore, EOPSS also appoints DCJIS as it designee to sign this Agreement on behalf of both DCJIS and EOPSS.

4.0 Scope

This Agreement is applicable to all sworn and non-sworn employees, contractors, interns, volunteers, and information technology support staff of all criminal justice and public safety agencies in the Commonwealth of Massachusetts who utilize or otherwise have access to any Public Safety Data Enterprise Application, software application, system or network maintained, or managed by EOPSS and/or DCJIS.

Public Safety Data Enterprise Applications within the scope of this agreement include the following:

Automated License Plate Reader (ALPR) technology is a system that allows for the automatic recognition of license plates by a portable or stationary unit. The license plate information is then compared against a locally stored list of plates called the CJIS-NCIC Hotfile database which consists of license plate numbers associated with suspended or revoked licenses, stolen vehicles, AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Be On Look Out, and Wanted or Missing Person broadcasts where a license plate is included.

CopLink is a crime analytics platform application maintained by the Massachusetts State Police Fusion Center that allows for the inter-agency storage and sharing of various documents and information.

EOPSS Data Cross Tracking System is a data collection and reporting system for criminal justice agencies and the Trial Court, to capture and report information on offenders and to report information relative to recidivism rates.

EOPSS National Incident Based Reporting System (NIBRS) Data Collection is a data collection and reporting system that criminal justice agencies submit incident and arrest data to in compliance with the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) standards.

My License Office (MLO) is an application that allows for the retrieval and use of Massachusetts' driver's license photos for various reasons, including professional licenses and identification cards.

The **Victim Notification Registry (VNR)** is the electronic application that allows for the registration of crime victims to receive notification of an offender's release from incarceration and certain CORI information.

This agreement may be amended from time to time to update the listing of Public Safety Data Enterprise Applications within the scope of this agreement.

5.0 Duration of Agreement

This Agreement is in effect until modified or cancelled by EOPSS and/or DCJIS. Each Agency Head shall sign off on a copy of this Agreement as a condition of access to the systems and networks operated, maintained, or managed by the EOPSS and/or DCJIS. In addition, each Agency Head will sign off on a copy of the Companion System Agreement for each system for which such an agreement exists. An original, signed copy of this Agreement, along with original, signed copies of any Companion System Agreements, will be kept on file at the DCJIS. The Agency Head shall maintain a copy of the signed agreements. Facsimile and electronic signatures are acceptable as originals.

The Agency Head also agrees to execute a new Global Justice and Public Safety User Agreement and all relevant Companion System Agreements in accordance with 803 CMR 7.06 whenever there are changes to the Agency Head, the CJIS Representative, the backup CJIS Representative, or the CJIS Technical Representative. The new Agreement(s) is/are to be executed within ten (10) business days of the effective date of the change(s) necessitating a new Agreement(s). Original, signed copies of the newly executed Agreement(s) will be forwarded to the DCJIS within ten (10) days of execution.

6.0 Definitions

Authorized User
A sworn or non-sworn justice or public safety employee, contractor, intern, volunteer, or IT support staff member who has been authorized by his/her agency head to access any software application, system, network, or CJI operated, maintained, or managed by the DCJIS.

Companion System Agreement
An addendum or "rider" to this Agreement. Each Companion System Agreement establishes rules and protocols for contributing CJI to, or accessing, using, or disseminating CJI from, a specific system or database operated, maintained, or managed by the DCIJS.

Criminal Intelligence System
A system that stores detailed intelligence or investigative information on the suspected criminal activities of subjects and/or which stores only information designed to identify individuals or organizations that are the subject of an inquiry or analysis.

Criminal Justice Information (CJI)
CJI is defined as all data obtained from or through the CJIS or companion public safety data enterprise application necessary for law enforcement agencies to perform their missions. CJI includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Information System (CJIS) Representative
The CJIS Representative serves as the primary agency point of contact for the DCJIS. Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS- sponsored meetings, seminars, and conferences.

Criminal Justice Information System (CJIS) Backup Representative
The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. The Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Rep representative be unable to perform those duties and responsibilities for any reason.

Criminal Justice Information System (CJIS) Technical Representative
The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

Criminal Justice Information System (CJIS) User-Access Model
A single-identity management model used to authenticate users of the software applications, systems, and networks operated, maintained, or managed by the DCJIS.

Public Safety Data Enterprise Application
A software application which criminal justice and public safety agencies use to contribute CJI to, or to access CJI from, databases or systems maintained by or accessed through the DCJIS.

Non-Contributing Agency
An agency that may access CJI from, but which does not contribute CJI to, a database or system operated, maintained, or managed by the EOPSS or DCJIS.

Source Agency
The agency that originally recorded and contributed data to a database or system operated, maintained, or managed by EOPSS or DCJIS.

7.0 Transaction Logs

An audit log of all transactions made by CJIS user agencies is maintained by the DCJIS and EOPSS for systems maintained by EOPSS or DCJIS. This log records the identity of the individual user and agency accessing the system, the date and time of access, and the data entered into, or retrieved from, any database or system operated, maintained, or managed by the EOPSS or DCJIS.
An Agency Head may request a report of all transactions initiated by the users of his/her agency. All report requests must be submitted in writing to the DCJIS.

The DCJIS CSO, at his/her discretion, may, at any time, authorize additional audits of all databases and systems operated, maintained, or managed by the EOPSS or DCJI S.

8.0 Audits of CJI Users

The DCJIS will conduct audits of all agencies, both criminal justice/public safety and non-criminal justice, accessing or using the CJI stored within, or obtained through, the databases, systems, and networks operated, maintained, or managed by the DCJIS. The purpose of these audits is to ensure the integrity and security of the CJI, applications, and systems, to investigate potential inappropriate use of these resources, and to identify potential training needs. Each CJIS user agencies will be audited at least on a triennial basis (once every 3 years).

9.0 Public Safety CJI, System, and Network Usage Restrictions

Use of any CJI obtained from or through an application, database, system, or network operated, maintained, or managed by the EOPSS or DCJIS is limited to authorized criminal justice purposes within the scope of a user's employment and official duties.

EOPSS and DCJIS resources may not be used for personal gain or for personal use, or to assist another individual or entity that is not authorized to access, use, or receive CJI from these resources. Criminal intelligence systems may also be subject to 28 CFR Part 23. Where the provisions of this Agreement or its addenda conflict with 28 CFR Part 23, 28 CFR Part 23 shall supersede this Agreement and its addenda.

10.0 Misuse

An Agency Head is responsible for investigating all alleged incidents or allegations of misuse of any CJI or database, system, or network operated, maintained, or managed by EOPSS or DCJIS. If an Agency Head determines that someone within his/ her agency has misused any of these resources, he/she must, within 10 business days, notify the DCJIS CSO in writing of the circumstances surrounding the misuse, of the actions taken, or to be taken, to address and correct the misuse, and of the policy(ies) and procedures to be implemented to prevent future misuse. The DCJIS CSO may suspend or revoke access to any or all databases or systems operated, maintained, or managed by the DCJIS for the individual(s) involved in the misuse.

Misuse of any EOPSS or DCJIS provided CJI or resource may result in individual loss of access to the resources, agency loss of access to the resources, and/or state and federal civil and criminal penalties, if applicable. Users are also subject to the rules and regulations of their respective agency.

11.0 Access to EOPSS and DCJIS Resources

Sworn and non-sworn justice and public safety employees, as well as the employees of non-criminal justice agencies, may be granted access to one or more DCJIS applications, systems, and networks as authorized by the Agency head.

Each individual accessing an EOPSS or DCJIS resource will be assigned a unique user identifier (User ID) and initial password. The individual will be required to change his/her password when logging into a resource for the first time. When possible, the same User ID and Password will enable a user to access multiple EOPSS and DCJIS resources. However, some applications may require a separate log in and/or a different User ID and Password.

All passwords used to access an EOPSS or DCJIS resource will meet the DCJIS and FBI security requirements in effect at the time the password is created/changed.

Authorized users shall not share their passwords and user identifications with any other individual. Each authorized user shall be responsible for all transactions conducted with his or her user identification and password.

Agencies are responsible for notifying the EOPSS or DCJIS, in writing, when a user is no longer authorized to access and EOPS or DCJIS resource. EOPSS or DCJIS will terminate or suspend user access depending on the user's status within his/her respective agency.

User IDs and passwords shall be reviewed by each agency on an annual basis. The Agency Head and agency CJIS Representative shall be responsible for this review. The purpose of this review is to confirm the continued authorization of all individuals accessing DCJIS resources. The Agency Head and CJIS Representative shall annually certify the accuracy of his/her agency's authorized user list to the DCJIS CSO.

12.0 Ownership of CJI Contained Within EOPSS or DCJIS Databases and Systems

The Source Agency will maintain ownership of, and responsibility for, the CJI it enters or modifies within any database or system operated, maintained, or managed by the EOPSS or DCJIS.

The Source Agency will exercise due diligence to ensure that the CJI it enters is current, complete, and accurate. Each Source Agency is also responsible for ensuring that the CJI it contributes is in compliance with all federal, state, and local laws.

User agencies shall communicate any errors found in CJI contained in any database or system operated, maintained, or managed by the DCJIS to the Source agency for that CJI as well as to the EOPSS or DCJIS.

13.0 Dissemination of CJI

CJI contained within, or obtained through, any database, system, or network operated, maintained, or managed by the EOPSS or DCJIS shall only be disseminated to other authorized agencies and individuals. In addition, the CJI obtained within, or obtained through, any DCJIS resource shall only be used for authorized criminal justice purposes.

14.0 Public Records

Records maintained within the databases and systems operated, maintained, or managed by the EOPSS or DCJIS are subject to the Massachusetts Public Records Law as defined in M.G.L. c. 4, s. 7(26).

All responses to public record requests for information contained in an EOPSS or DCJIS resource shall be referred to the Agency that contributed the relevant information for its response as the custodian of the record(s).

The EOPSS or DCJIS CSO may respond to a public records request for statistical data drawn from an EOPSS or DCJIS resource.

15.0 Data Submission and Retention Policy

Source Agencies shall contribute data to each EOPSS or DCJIS database or system pursuant to the schedule established in the Companion System Agreement for that database or system, if applicable. Companion System Agreements are attached to this Agreement as Addenda.

Data maintained in an EOPSS or DCJIS database(s) and system(s) shall be retained pursuant to the schedule established in the Companion System Agreement for that respective system, if applicable.

16.0 Data Submission Standards

For each system that requires the contribution of data by Source Agencies, those Agencies shall submit at least the minimum set of data as established in the guidelines or any Companion System Agreement if required, for the respective subject application.

17.0 Designation of an Agency Representatives

CJIS Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the EOPSS or DCJIS shall appoint a CJIS Representative. The CJIS Representative serves as the primary agency point of contact for the EOPSS and DCJIS. Responsibilities include ensuring that all EOPSS and DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the EOPSS or DCJIS or who use the CJI obtained from or through those systems and networks, and attending all EOPSS or DCJIS- sponsored meetings, trainings, seminars, and conferences.

Backup CJIS Representative*:*
Each agency that accesses or uses CJI obtained from or through the syst ems or networks operated, maintained, or managed by the DCJIS shall also appoint a Backup CJIS Representative. The Backup CJIS Representative shall be the EOPSS and DCJIS' secondary point of contact for the agency. In addition, the Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

CJIS Technical Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Technical Representative. The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

18.0 Technical Support

The Executive Office of Public Safety and Security (EOPSS) Office of Technology and Information Services (OTIS) shall provide technical support services for all applications, databases, systems, and networks, operated, maintained, or managed by the EOPSS or DCJIS.

19.0 Internal Agency Policies

Each agency obtaining CJI either directly from, or through, an application, database, system, or network operated, maintained, or managed by the EOPSS or DCJIS shall draft

and adopt internal policies to inform and ensure that agency authorized users have read and agree to comply with the provisions of this Agreement and its Addenda .

20.0 Termination of Access

An agency may request termination of its access to one or more EOPSS or DCJIS resources by providing a written request to the DCJIS CSO.
The DCJIS CSO may also terminate access to a DCJIS resource pursuant to the terms of a Companion System Agreement.

21.0 Amendments

Any change in the provisions of this Agreement or in the provisions of a Companion System Agreement shall be incorporated by a written amendment approved by the EOPSS and DCJIS CSO.

22.0 Global Justice and Public Safety User Agreement Signoff

By signing this Agreement, the Agency Head acknowledges he/ she has read and understood its provisions and that he/she will comply with its terms and conditions.

_____
_____
Agency Head Name/Title

Commissioner, Department of Criminal Justice Information Services

_____
Agency

_____
_____
Agency Head Signature

DCJIS Commissioner Signature

_____
_____
Date

Date

MEMORANDUM OF UNDERSTANDING

USE OF A CRIMINAL JUSTICE AGENCY CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS) ROUTER and SWITCH BY A NON-CRIMINAL JUSTICE AGENCY

Once executed by all parties, this MOU must remain on file with the Host, the User, and the DCJIS.

This Memorandum of Understanding (MOU) is entered into this _____day of_____, 20___ by and between _____, a criminal justice agency, hereafter referred to as the **Host,** and _____, a non-criminal justice agency, hereafter referred to as the **User**.

This MOU defines the terms, conditions, and mutual responsibilities of the parties hereto, for the purpose of enabling the User to access the Host's/User's internal Computer-Aided Dispatch (CAD) system and/or Records Management System (RMS) via mobile data terminals utilizing the Host's CJIS router and switch. This MOU incorporates by reference, and operates in conjunction with, the standard Massachusetts CJIS User Agreement, which includes agreement by the Host to adhere to the Federal Bureau of Investigation's (FBI's) Criminal Justice Information System (CJIS) Security Policy (hereinafter, the CSP). It is the Host's responsibility to ensure that its CJIS User Agreement with the DCJIS is current and on file at the DCJIS Support Services Unit and with its Agency Head.

The User and Host agree:

a. To be bound by the conditions of this MOU and to notify each other and the DCJIS in the event that any of the conditions stated in this Agreement change in the future;
b. To execute a new MOU with the DCJIS once every two (2) years as long as the Host/User relationship continues;
c. To notify the DCJIS of pending termination immediately, as provided in the final paragraph of this MOU;
d. To develop and maintain a written agreement that includes a procedural statement that clearly identifies the responsibilities of each agency;
e. **That calls for service to the DCJIS must be made by the Host criminal justice agency;**
f. That a violation of this MOU shall be considered a violation of the CJIS User Agreement between the violating party(ies) and the DCJIS.

The Host understands that the use of the CJIS router and switch by a non-criminal justice agency is not standard protocol and that the DCJIS only agrees to this arrangement where such access is necessary to aid the User non-criminal justice agency in the performance of its official public safety duties.

The Host hereby agrees to only allow the User to utilize the CJIS router and switch to access User data systems in the performance of its public safety duties. Access to any CJIS or Criminal Offender Record Information (CORI) data systems is prohibited.

The Host hereby acknowledges an understanding of, and shall advise all its employees and user agency personnel of, the penalties relating to illegal actions with regard to criminal justice information, the Criminal Offender Record Information (CORI) Act as found in M.G.L. c. 6, § 167

et seq., the CJIS User Agreement, and the CSP.

The User agrees that the Host's CJIS router and switch will be used to access non-CJIS and/or non-CORI data only, which will aid in the performance of its official public safety duties, provided that the dissemination of such information would not be a violation of any laws or regulations of the United States or of the Commonwealth of Massachusetts.

Either the Host or the User may, upon thirty (30) days notice to the other party and to the DCJIS, in writing, cancel this MOU in its entirety. Upon determination that the Host or User has violated any law, rule, or regulation concerning criminal justice information or the use of the Host's CJIS router and/or switch, or violated the terms of this MOU, the Host or User, in cooperation with the DCJIS, reserves the right to terminate this MOU with or without notice. The DCJIS may terminate this MOU at any time and without notice.

USER: _____ **HOST:** _____

*By: _____ *By: _____

Title: _____ Title: _____

Date: _____ Date: _____

Print Name: _____ Print Name: _____

DCJIS:

*By: _____

Title: _____Commissioner_____

Date: _____

Print Name: ___Jamison Gagnon_____

***Signature of person who is legally authorized to sign for the agency.**

MEMORANDUM OF UNDERSTANDING
CRIMINAL JUSTICE AGENCY
MOBILE DATA SHARING HOST/USER GUIDELINES

Once executed by all parties, this MOU must remain on file with the Host, the User, and the Department of Criminal Justice Information Services (DCJIS).

This Memorandum of Understanding (MOU) is entered into this _____day of_____, 20_____ by and between _____, a criminal justice agency hereafter referred to as the **Host,** and _____, a criminal justice agency hereafter referred to as the **User**.

This MOU is intended to define the terms, conditions, and mutual responsibilities of the parties hereto, for the purpose of enabling the User access, via the User's mobile data terminals, to the Massachusetts Criminal Justice Information System (CJIS), including access to Registry of Motor Vehicle (RMV) data and images, to FBI CJIS systems, including the National Crime Information Center (NCIC), and to the International Justice and Public Safety Network (Nlets), utilizing the Host's server, the Host's CJIS router, and other hardware and software necessary to operate wireless devices. This MOU incorporates by reference, and operates in conjunction with, the Massachusetts CJIS User Agreement and the FBI CJIS Security Policy. Both parties agree to adhere to all Massachusetts CJIS policies and to the policies of both the FBI and Nlets.

The User and Host agree:

g. To be bound by the conditions of this MOU and to notify each other and the DCJIS in the event that any of the conditions stated in this Agreement change in the future.
h. To execute this MOU with the DCJIS biennially as long as the Host/User relationship continues.
i. To notify the DCJIS of pending relationship termination immediately, as provided in the final paragraph of this MOU.
j. To develop and maintain a separate written agreement which includes procedures that clearly identifies the responsibilities of each agency when a mobile/wireless server is not functioning, and which department is responsible for managing the vendor response process. This agreement must detail the maintenance process and identify (1) who is responsible for contacting the DCJIS for service issues and (2) who is responsible for costs associated with the server and usage.
k. **That calls for service to the DCJIS must be made by the Host Agency;** and
l. That a violation of this MOU shall be considered a violation of the CJIS User Agreement between the violating party and the DCJIS.

The Host understands that the use of the Host's server by another criminal justice agency is not standard protocol and that the DCJIS only agrees to this arrangement where such access is necessary to aid the User criminal justice agency in the performance of the User's official criminal justice duties. The Host hereby agrees to:

d. Allow the User to utilize the Host's base system for access to any and all available information on the CJIS, RMV, FBI, and Nlets systems, via approved wireless devices, provided that the dissemination of such information would not be a violation of any laws or regulations of the United States or of the Commonwealth of Massachusetts.
e. Provide assistance in the furtherance of criminal justice information (CJI) processing and communications through record inquiry, message transmittals, or record entries in

keeping with all standards, and further agrees to limit access to such information to authorized employees of the User; and

f. Maintain an automated log of inquiries or transactions made by any of the User's wireless devices. The log must include the identification of the specific wireless device from which the inquiry was made, the operator of the device, the operator's department, and the date and time of the inquiry or transaction. Each log entry must be maintained by the Host for a minimum of one year and must be provided to the DCJIS and to the FBI upon request.

The User hereby acknowledges that it understands, and shall advise all its employees of, the penalties relating to unauthorized access to, or dissemination of CJI as defined in the Criminal Offender Record Information (CORI) Act (M.G.L. c. 6, § 167 et seq.), in 803 C.M.R. 2.00-9.00 et seq., in 28 CFR, in the CJIS User Agreement, and in the FBI CJIS Security Policy. The User agrees:

e. To abide by all laws of the United States and the Commonwealth of Massachusetts, as well as by the rules and regulations of the responsible administrative agencies, including the DCJIS as the FBI CJIS Systems Agency (CSA), and the FBI.
f. To abide by the standards and conditions of the CJIS User Agreement concerning the security, entry, collection, storage, verification, retrieval, access, and dissemination of CJI.
g. That the Host's system will be used for inquiries only; and
h. That all its personnel with access to wireless devices that will utilize the Host's base system have been trained, tested, and certified as required by the DCJIS and the FBI.

Either the Host or the User may, upon thirty days written notice to the other party and to the DCJIS, cancel this MOU in its entirety. Upon determination that the User has violated the terms of this MOU, the Host, in cooperation with the DCJIS, reserves the right to terminate this MOU with or without notice. The DCJIS may terminate this MOU at any time and without notice.

In witness thereof, the above-named parties have signed this document in full agreement on this _____day of_____, 20___.

USER AGENCY: _____ HOST AGENCY: _____

By: _____ By: _____
(Signature of Chief/Agency Head) (Signature of Chief/Agency Head)

Title: _____ Title: _____

Date: _____ Date: _____ ____
CJIS Systems Officer: _____ Date: _____

Jamison R. Gagnon

MEMORANDUM OF UNDERSTANDING
CRIMINAL JUSTICE AGENCY
MOBILE DATA SHARING HOST/USER GUIDELINES

Once executed by all parties, this MOU must remain on file with the Host, the User, and the Department of Criminal Justice Information Services (DCJIS).

This Memorandum of Understanding (MOU) is entered into this _____day of_____, 20_____ by and between _____, a criminal justice agency hereafter referred to as the **Host,** and _____, a criminal justice agency hereafter referred to as the **User**.

This MOU is intended to define the terms, conditions, and mutual responsibilities of the parties hereto, for the purpose of enabling the User access, via the User's mobile data terminals, to the Massachusetts Criminal Justice Information System (CJIS), including access to Registry of Motor Vehicle (RMV) data and images, to FBI CJIS systems, including the National Crime Information Center (NCIC), and to the International Justice and Public Safety Network (Nlets), utilizing the Host's server, the Host's CJIS router, and other hardware and software necessary to operate wireless devices. This MOU incorporates by reference, and operates in conjunction with, the Massachusetts CJIS User Agreement and the FBI CJIS Security Policy. Both parties agree to adhere to all Massachusetts CJIS policies and to the policies of both the FBI and Nlets.

The User and Host agree:

m. To be bound by the conditions of this MOU and to notify each other and the DCJIS in the event that any of the conditions stated in this Agreement change in the future.
n. To execute this MOU with the DCJIS biennially as long as the Host/User relationship continues.
o. To notify the DCJIS of pending relationship termination immediately, as provided in the final paragraph of this MOU.
p. To develop and maintain a separate written agreement which includes procedures that clearly identifies the responsibilities of each agency when a mobile/wireless server is not functioning, and which department is responsible for managing the vendor response process. This agreement must detail the maintenance process and identify (1) who is responsible for contacting the DCJIS for service issues and (2) who is responsible for costs associated with the server and usage.

q. **That calls for service to the DCJIS must be made by the Host Agency;** and
r. That a violation of this MOU shall be considered a violation of the CJIS User Agreement between the violating party and the DCJIS.

The Host understands that the use of the Host's server by another criminal justice agency is not standard protocol and that the DCJIS only agrees to this arrangement where such access is necessary to aid the User criminal justice agency in the performance of the User's official criminal justice duties. The Host hereby agrees to:

g. Allow the User to utilize the Host's base system for access to any and all available information on the CJIS, RMV, FBI, and Nlets systems, via approved wireless devices, provided that the dissemination of such information would not be a violation of any laws or regulations of the United States or of the Commonwealth of Massachusetts.

h. Provide assistance in the furtherance of criminal justice information (CJI) processing and communications through record inquiry, message transmittals, or record entries in keeping with all standards, and further agrees to limit access to such information to authorized employees of the User; and
i. Maintain an automated log of inquiries or transactions made by any of the User's wireless devices. The log must include the identification of the specific wireless device from which the inquiry was made, the operator of the device, the operator's department, and the date and time of the inquiry or transaction. Each log entry must be maintained by the Host for a minimum of one year and must be provided to the DCJIS and to the FBI upon request.

The User hereby acknowledges that it understands, and shall advise all its employees of, the penalties relating to unauthorized access to, or dissemination of CJI as defined in the Criminal Offender Record Information (CORI) Act (M.G.L. c. 6, § 167 et seq.), in 803 C.M.R. 2.00-9.00 et seq., in 28 CFR, in the CJIS User Agreement, and in the FBI CJIS Security Policy. The User agrees:

i. To abide by all laws of the United States and the Commonwealth of Massachusetts, as well as by the rules and regulations of the responsible administrative agencies, including the DCJIS as the FBI CJIS Systems Agency (CSA), and the FBI.
j. To abide by the standards and conditions of the CJIS User Agreement concerning the security, entry, collection, storage, verification, retrieval, access, and dissemination of CJI.
k. That the Host's system will be used for inquiries only; and
l. That all its personnel with access to wireless devices that will utilize the Host's base system have been trained, tested, and certified as required by the DCJIS and the FBI.

Either the Host or the User may, upon thirty days written notice to the other party and to the DCJIS, cancel this MOU in its entirety. Upon determination that the User has violated the terms of this MOU, the Host, in cooperation with the DCJIS, reserves the right to terminate this MOU with or without notice. The DCJIS may terminate this MOU at any time and without notice.

In witness thereof, the above-named parties have signed this document in full agreement on this _____day of_____, 20___.

USER AGENCY: _____ **HOST AGENCY: _____**

By: _____ By: _____
(Signature of Chief/Agency Head) (Signature of Chief/Agency Head)

Title: _____ Title: _____

Date: _____ Date: _____

CJIS Systems Officer: _____ Date: _____

Jamison R. Gagnon

MEMORANDUM OF UNDERSTANDING
NON-CRIMINAL JUSTICE AGENCY ACCESS TO A
CRIMINAL JUSTICE AGENCY RECORDS MANAGEMENT SYSTEM

Once executed by all parties, this MOU must remain on file with the Host, the User, and the Department of Criminal Justice Information Services (DCJIS).

This Memorandum of Understanding (MOU) is entered into this _____day of_____, 20_____ by and between _____, a criminal justice agency hereafter referred to as the **Host,** and _____, a non-criminal justice agency hereafter referred to as the **User**.

This MOU is intended to define the terms, conditions, and mutual responsibilities of the parties hereto, for the purpose of enabling the User to access the Host's internal Records Management Systems (RMS). . This MOU incorporates by reference, and operates in conjunction with, the Massachusetts Criminal Justice Information System (CJIS) User Agreement and the FBI CJIS Security Policy. It is the Host's responsibility to ensure that its CJIS User Agreement with the DCJIS is current and on file at the DCJIS.

The User and Host agree:

a. To be bound by the conditions of this MOU and to notify each other and the DCJIS in the event that any of the conditions stated in this Agreement change in the future.
b. To execute an MOU with the DCJIS biennially as long as the Host/User relationship continues.
c. To notify the DCJIS of pending relationship termination immediately, as provided in the final paragraph of this MOU.
d. To develop and maintain a separate written agreement which includes procedures that clearly identify the responsibilities of each agency.
e. **That calls for service to the DCJIS must be made by the Host Agency;** and
f. That a violation of this MOU shall be considered a violation of the CJIS User Agreement between the violating party and the DCJIS.

The Host understands that the use of the state CJIS router and switch by a non-criminal justice agency is not standard protocol and that the DCJIS only agrees to this arrangement where such access is necessary to aid the User agency in the performance of its official public safety duties. Therefore, the Host hereby agrees to only allow the User agency to utilize the state CJIS router and switch to access Host data systems in the performance of its public safety duties. Access to any CJIS, FBI, or Criminal Offender Record Information (CORI) data or systems is prohibited.

The Host hereby acknowledges that it understands and shall advise all its employees and User personnel of the penalties relating to unauthorized access to, or dissemination of, CJI as defined in the Criminal Offender Record Information (CORI) Act (M.G.L. c. 6, § 167 et seq.), in 803 C.M.R. 2.00-9.00 et seq., in 28 CFR, in the CJIS User Agreement, and in the FBI CJIS Security Policy.

The User agrees that the Host's CJIS router and switch will be used to access non-CJIS and/or non-CORI data only to aid in the performance of its official public safety duties, provided that the dissemination of such information would not be a violation of any laws or regulations of the United States or of the Commonwealth of Massachusetts.

Either the Host or the User may, upon thirty days written notice to the other party and to the DCJIS, cancel this MOU in its entirety. Upon determination that the User has violated the terms of this MOU, the Host, in cooperation with the DCJIS, reserves the right to terminate this MOU with or without notice. The DCJIS may terminate this MOU at any time and without notice.

In witness thereof, the above-named parties have signed this document in full agreement on this _____day of_____, 20___.

USER AGENCY: _____ **HOST AGENCY: _____**

By: _____ By: _____
(Signature of Chief/Agency Head) (Signature of Chief/Agency Head)

Title: _____ Title: _____

Date: _____ Date: _____ ____

CJIS Systems Officer: _____ Date: _____
Jamison R. Gagnon

{PLACE ON AGENCY LETTERHEAD}

This agreement is entered into this _____ day of _____ 20___ by and between the _____, hereafter referred to as the Agency, and the _____, hereafter referred to as the User. This Agreement identifies the duties and responsibilities of both the Agency and the User.

Agency Responsibilities:

The Agency hereby agrees to provide the User with access to all CJIS, FBI CJIS, and Nlets data and services available to the Agency, subject to the limits, if any, indicated below, which will aid the User in the performance of its official law enforcement or criminal justice duties, so long as the provision of these services and information would not be a violation of State or Federal laws, regulations, and/or policies.

(Include this section ONLY if the Agency and User agree to the provision of limited services)

Services to be provided:

The Agency agrees to provide the following to the User:

- {List the specific services or data to be provided here}

The Agency agrees to provide assistance to the User as may be requested in the furtherance of criminal justice information processing and communications through record inquiry, message transmittals, and/or record entry and maintenance in keeping with all standards and policies, and further agrees to limit access to services and CJI to authorized employees of the User.

User Responsibilities:

The User agrees to abide by all laws of the United States, the Commonwealth of Massachusetts, and the rules, policies, and regulations of the responsible administrative agencies concerning the collection, storage, retrieval, and dissemination of criminal justice information (CJI). The User specifically agrees to follow the rules, policies, and operating standards contained within the CJIS User Agreement and the FBI CJIS Security Policy. The User agrees that the services and CJI provided to it under this agreement will only be requested and used for authorized criminal justice purposes.

The User further agrees that it will only disseminate CJI to other legally authorized law enforcement and criminal justice personnel, or to other legally authorized individuals and entities. The User will log all such disseminations in a Secondary Dissemination Log.

The User will ensure that all personnel authorized to access CJIS, FBI CJIS, and Nlets services and information pursuant to this agreement are required to review the CJIS User Agreement and the FBI CJIS Security Policy. The User will retain an acknowledgement from each such authorized individual in its files. In addition, the User will ensure that each authorized individual is trained, tested, and certified within 6 months of employment and then once every two years thereafter. The User will notify the Agency and the DCJIS, in writing, within 5 days of any hires, transfers, or terminations of personnel authorized to access CJI pursuant to this agreement.

The User hereby acknowledges understanding, and shall advise all its employees, of the penalties relating to improper or illegal access to, or use of, CJI, including Criminal Offender Record Information (CORI) and criminal history record information (CHRI).

Nothing in this agreement shall be construed so as to give authority to any person, agency, corporation, or other legal entity to invade the privacy of any individual, as defined by State and Federal law.

Either the Agency or the User may, upon thirty (30) days written notice to the other party, cancel this agreement in its entirety. Either the Agency or User, after consulting with the Department of Criminal Justice Information Services, reserves the right to terminate this agreement with or without notice upon determining that the other party has violated any law, rule, or regulation concerning access to, or use of, CJI or has otherwise violated the terms of this agreement.

IN WITNESS WHEREOF, the above-named parties have set their hand and seal this _____ day of _____ 20___, in full agreement with this **Management Control Agreement** document, and so designate by execution on the following appropriate lines.*

Pursuant to the CJIS Security Policy Version 5, Sections 3.2.2 and 5.1, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and termination of personnel.
(3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
(5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

USER: _____ AGENCY: _____

"Responsibility for management of security control shall remain with the criminal justice agency."

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

_____ _____
John Smith, CIO Date
Any State Department of Administration

_____ _____
BY: _____ BY: _____

TITLE: _____ TITLE: _____

DATE: _____ DATE: _____

*This agreement must be signed by the Station Commander, Director, Chief, or head of the agencies which are parties to this agreement.

This Agreement is not valid until signed by the FBI CJIS Systems Officer (CSA) of the DCJIS.

APPROVED: _____ DATE: _____

The Agency must forward a copy of this Agreement to the following:

Department of Criminal Justice Information Services
CJIS Support Services Unit
200 Arlington St., Suite 2200
Chelsea, MA 02150

Joan Brown, CIO
(Criminal Justice Agency)

Date

MASSACHUSETTS CJIS USER AGREEMENT

1. User Agreement Introduction

1.1 This User Agreement sets forth the mutual responsibilities of the Department of Criminal Justice Information Services (DCJIS) as the CJIS Systems Agency (CSA) for the Commonwealth of Massachusetts and each user agency of the CJIS as it relates to the operation, maintenance and security of the systems and services provided. Authority for this agreement is granted by 803, Code of Massachusetts Regulations (CMR), 7.05, in accordance with M.G.L c. 6, §§ 168, 174 and 175, and 28, Code of Federal Regulations (CFR), 20.1.

1.2 The department head of each user agency shall submit a new User Agreement to the CJIS Support Services (CSS) Unit bi-annually, or within 10 days upon the designation of a new CJIS representative, back-up representative, or appointment of a new agency head. Said User Agreement will be due on March 1st of the designated year to renew. The CSS Unit will send a message on or about January 31st bi-annually, and once a week thereafter, to all user agencies reminding them to renew their User Agreements.

2. General Introduction

2.1 **Department of Criminal Justice Information Services (DCJIS)** – As an Executive Office of Public Safety and Security agency, the Massachusetts Department of Criminal Justice Information Services (DJCIS) provides twenty-four hour support, seven days a week to local, state, and national public safety agencies. Our Criminal Justice Information Systems (CJIS) Division operates a secure public safety data center and network that provides the critical infrastructure that supports information sharing and interoperability for the Commonwealth's criminal justice and law enforcement communities.

2.2 **Criminal Justice Information System (CJIS)** – The CJIS is the computerized network, services and applications that offer law enforcement and criminal justice agencies within the state and across the nation secure access 24 hours per day 7 days a week to state and interstate criminal history record information, protective orders, missing and wanted person files, drivers' license and motor vehicle information, firearms licensing and gun sales transactions and other critical criminal justice information. The CJIS provides access to the Board of Probation (BOP), the FBI's National Crime Information Center (NCIC) and Interstate Identification Index (III), the International Justice and Public Safety Network (Nlets), the Massachusetts Warrant Management System (WMS), and the Automated Licensing and Registration System (ATLAS) maintained by the Registry of Motor Vehicles (RMV).

2.3 The DCJIS is the CJIS Systems Agency (CSA) for the Commonwealth of Massachusetts. In this capacity, the DCJIS is responsible to the FBI CJIS Division for ensuring that user agencies are provided with twenty-four (24) hour access to national criminal justice information files such as missing and wanted persons, criminal history, Integrated Automated Fingerprint Identification System (IAFIS) and the Convicted Sexual Offender Registry File (CSORF).

2.4 To fulfill this responsibility the CJIS Support Services (CSS) Unit of the DCJIS provides the following services to its users:

- Policy review of matters pertaining to Massachusetts Criminal Offender Record Information (CORI and BOP files), NCIC, Interstate Identification Index (III), Nlets, state and national warrant, protective orders convicted sexual offender files and other enterprise applications available via CJIS;

- Training and certification in the use of the CJIS enterprise application to include BOP, WMS, RMV, NCIC and Nlets and the Massachusetts Instant Record Check System (MIRCS) application;

- Quality Control – It is the responsibility of the CSS Unit to ensure each user agency adheres to the NCIC policies in regards to maintaining the accuracy and integrity of records in the CJIS and NCIC systems.

- Auditing – A compliance audit is conducted approximately every three years to verify that user agencies are adhering to CJIS and NCIC policies and regulations. The purpose of the CJIS audit is to ensure that records in the system are accurate, active and timely, ensure that training is conducted, security standards are met, and to verify that the proper documentation is maintained and available for DCJIS and FBI NCIC auditing purposes;

- Off-line searches – For investigative purposes, at the request of a criminal justice agency, the CSS Unit may conduct an off-line search of the CJIS to obtain data regarding a person, vehicle or article that has been the subject of a previous CJIS query(s). This data is used by the requesting agency to determine what specific person(s) or what specific CJIS workstation(s) has run a query on the person/article of interest. Requests may also be used to gather information on a specific CJIS user or CJIS workstation.

Incorporated References & NCIC and State files Available to users

The following documents are incorporated by reference and made part of this agreement:

- *Interstate Identification Index Operational and Technical Manual, NCIC 2000 Operating Manual*; and National Incident-Based Reporting System Volumes 1-4;
- Minutes of the FBI CJIS Advisory Policy Board meetings;
- *Bylaws for the CJIS Advisory Policy Board* and *Working Groups*;
- *Title 28, Code of Federal Regulations, Part 20*
- FBI *CJIS Security Policy* to include all elements of the *NCIC Computerized Criminal History Program Background, Concept and Policy*;
- *A Policy and Reference Manual*;
- Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information, NCIC Standards, and UCR Standards, as recommended by the CJIS Advisory Policy Board;
- Other relevant documents to include *NCIC Technical and Operational Update, CJIS Information Letter*, etc;

- Federal Information Processing System (FIPS) Publication 140-2;
- Public Law 92-544;
- 42 U.S.C. § 1437(d);
- FBI Electronic Fingerprint Transmission Specification (EFTS) - CJIS –RS-0010 v.7;
- Massachusetts Electronic Fingerprint Transmission Specification (MEFTS) v.7;
- M.G.L c. 6, §§ 167-178B, M.G.L. c. 121B, M.G.L. c. 263, § 1A, M.G.L. c. 94C, § 45, M.G.L. c. 127, §§ 23 & 28, M.G.L. c. 6A, § 18 ¾,;
- **803, Code of Massachusetts Regulations, Department of Criminal Justice Information Services;;**

The following NCIC or state files are available when direct access is authorized:

Vehicle File
Felony Vehicle File
License Plate File
Part File
Wanted Person File
Missing Person File
Unidentified Person File
Security File
Gun File
Article File
(BOP) Massachusetts Firearms License File
Transaction (Legacy and MIRCS)
Massachusetts Registry of Motor Vehicle
Investigative License and Registration Files
Department of Correction Inmate Release
Bulletin Program (CJIS Extranet)
Juvenile Lock Up Program
Suicide Risk File
Foreign Fugitive File
US Secret Service Protective File
Protective Order File
Deported Felon File
ATF Violent Felon File
Interstate Identification Index (III)
INS Service
MA Sex Offender Registry
MA Criminal History Records
Massachusetts Gun Sales
Database (Legacy and MIRCS)
Massachusetts CJIS RMV
Web Search (CJIS Extranet)
State Police Identification Section – ID
(CJIS Extranet)

3. Responsibilities/Expectations of User Agencies

3.1 Agency Head – The agency head is responsible for local management of the CJIS within his or her jurisdiction. Moreover, it is the responsibility of the agency head to develop formal written procedures regarding the operational use and security of CJIS to ensure compliance with CJIS and NCIC policy and regulations.

The agency head must also appoint a CJIS Representative(s), backup CJIS Representative(s), and a CJIS Technical Contact(s). The CJIS Technical Contact (s) should also be able to act as a security point of contact. Each representative chosen should be in a position to make decisions related to CJIS in a timely manner. Such information shall be provided to the DCJIS on the enclosed form bi-annually upon the renewal of the User Agreement and at any time CJIS Representatives and/or Technical Contact have changed.

NOTE: The CJIS Representative may serve as the technical and/or security

points of contact. See Appendix B for a more detailed list of responsibilities.

3.2 CJIS Representative(s) – The CJIS Representative(s) shall act as a liaison to DCJIS to ensure the proper administration of the CJIS at the agency level. The responsibilities of the CJIS Representative include:

- Ensuring that training is available to all authorized CJIS users within six (6) months of employment and every two (2) years thereafter.
- Providing certificates of achievement for the successful completion of training and a passing score on the appropriate CJIS examination. (Note: the appropriate examination depends on the hours of operation of the user agency as well as the access necessary for individual agency personnel. See Job description of CJIS Representative).
- Ensuring that the validation process is completed and is submitted to the CSS Unit on or before each month's specified due date.
- Proper password maintenance as required by CJIS security policy, including the disabling of accounts for individuals who have been suspended, fired, retired, or have voluntarily terminated their own employment.
- Attendance at the biannual Regional Working Group meetings. If neither the CJIS Representative nor his/her backup are able to attend, the agency head may designate another agency employee to be present.
- Timely responses to communications from the DCJIS.
- Distribution of publications to agency personnel as directed by the

DCJIS. See Appendix C for a more detailed list of responsibilities.

3.3 Technical Contact(s) – The CJIS Technical Contact(s) shall act as a liaison to DCJIS to ensure the proper technical/security administration of the CJIS at the local level. The responsibilities of the CJIS Technical Contact include:

- Ensuring that all problems experienced by user agencies regarding the CJIS and all CJIS equipment shall be reported to the Executive Office of Technology Services and Security (EOTSS) directly at (617) 660-4620 for troubleshooting and further escalation if necessary.

See Appendix D for a more detailed list of responsibilities.

The following are the duties and policies to which user agencies must be aware and follow in the administration of the CJIS.

3.4 Auditing – It is the intention of the CJIS Support Services (CSS) Unit to audit your agency once every three years via a mail survey or an in-person interview. The purpose of this audit is to ensure compliance with all Massachusetts CJIS and NCIC policies. Not adhering with any CJIS/NCIC policy will result in a letter of non-compliance and a time-frame to rectify the issue. If the problem is not resolved, your agency may be subject to penalty decided upon by the CJIS Systems Officer. See CJIS Operating Manual and NCIC 2000 Operating Manual for more information.

3.5 Criminal Ten-Print Record Submission – See M.G.L. c. 263, § 1A, M.G.L. c. 94C, § 45. M.G.L.
c. 127, § 23, and M.G.L. c. 127, § 28.

3.6 Dissemination of Criminal Justice Information:

3.6.1 Maintenance of criminal offender record information in electronic format; accessibility via world wide web; eligibility for access to database; use and dissemination of criminal offender record information - See M.G.L. c. 6, § 172.

3.6.2 Department of Criminal Justice Information Services – See 803 CMR 2.00 *et. seq.*

3.6.3 Proper access to and use of Criminal History Record Information (CHRI) – See the FBI
CJIS Security Policy.

3.6.4 Housing Authority Access of Criminal Offender Record Information (CORI) – See 803 CMR 5.00.

3.6.5 Housing Authority Access to Interstate Records – See 803 CMR 5.00 and 42 U.S.C. § 1437(d).

3.7 Electronic Fingerprint Record Submission:

3.7.1 Equipment and Procedures – See the Massachusetts Electronic Fingerprint Transmission Specification (MEFTS) and the FBI Fingerprint Transmission Specification (EFTS).

3.7.2 Equipment Maintenance – The agency head is responsible to ensure that all Electronic Fingerprint Submission equipment is subject to an up-to-date maintenance agreement with a DCJIS approved vendor.

3.7.3 Maintenance-Service Protocol – Problems experienced with the electronic fingerprinting equipment should be reported to the State Identification Section (SIS) at 508.358.3170.

3.8 Equipment and Maintenance - It is the responsibility of the agency head to ensure that all equipment connected to the CJIS Network has been approved by the DCJIS. In addition, the agency head shall be responsible for sustaining a maintenance agreement with a DCJIS approved vendor for each router, and switch the agency possesses.

Please do not touch, replace, relocate or reconnect any CJIS equipment without the consent of the DCJIS. Notification of any desired relocation, exchange, or replacement of a CJIS switch, or router, or any other CJIS related equipment must be made in writing to the CJIS Support Services (CSS) Unit a minimum of fifteen (15) business days prior to the planned relocation, exchange, or replacement. Moreover, if a problem arises with any CJIS related equipment, please contact EOTSS at 617-660-4620 before adjusting any devices or settings.

3.8.1 Mobile/Wireless Access to CJIS – Mobile/Wireless access to the CJIS is available through DCJIS approved equipment, provided that the FBI – NCIC & CJIS security requirements are met. A transaction log of all queries and responses must be maintained for a minimum of two years by the host agency, and made readily available upon the request of the DCJIS. See FBI *CJIS Security Policy* and the DCJIS CJIS Information Security Policies.

3.9 Hit Confirmation – Any agency which receives a record(s) in response to a CJIS or NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any adverse action. See NCIC 2000 Operating Manual.

3.10 Incident Reporting – A security incident is violation or a potential violation of the confidentiality, integrity and/or the availability of state/FBI CJIS data. If such an incident should occur, the agency head shall submit a fax, on agency letterhead, to the attention of the Department of Criminal Justice Information Services (DCJIS) Commissioner, CJIS Systems Officer/Information Security Officer to (617) 884-4601 within forty-eight hours with the following information:

- Date & Location of incident
- Systems affected
- Method of detection & Nature of Incident
- Description of the incident & Actions taken/resolution
- Date & Contact information for the agency

3.11 Locate – NCIC policy requires any agency, except the agency that entered the record, that apprehends or locates an individual or property to place a locate message on the record following confirmation with the original agency that entered the record. When placing a locate on a wanted person record, it is important to note that a locate should not be placed on a record if no extradition is indicated or the locating agency is outside the extradition limits set forth in the record. **Please note this also includes WMS and NCIC records.** See the NCIC 2000 Operating Manual.

3.12 Logging – Massachusetts CJIS User Agreement, based upon NCIC policy, requires that an automated log of all NCIC and III transactions be maintained for a minimum of two years. See the FBI *CJIS Security Policy.*

3.13 Memorandum of Understanding (MOU) – Any agency which provides certain CJIS services to one or more criminal justice agencies must execute a MOU with each agency to which it offers services. This agreement shall be implemented by the agency heads and must describe the services to be provided, outline the responsibilities of each party involved and be forwarded to the CSS unit within fourteen (14) day of its execution. Situations where an MOU shall be executed include, but are not limited to the following:

- Agencies which provide CJIS services to any non-terminal criminal justice agencies; and
- Agencies which provide CJIS services to any non-criminal justice agency (i.e. housing authority); and
- Agencies which provide CJIS services to any non-twenty-four (24) hour criminal justice agencies; and
- Any agency that provides CJIS services to one or more wireless devices (MDT/MDC) via a shared-server environment to another criminal justice agency;
- Any agency that submits arrest fingerprint cards, either manually or electronically to the State Police Identification Section on behalf of another agency.

3.14 Quality Assurance – Appropriate and reasonable procedures must be in place to ensure that records in the CJIS and NCIC systems are accurate, complete and valid. See the NCIC 2000 Operating Manual.

3.15 Screening – Pre-employment background screening must be conducted on all personnel who have authorized access to CJIS and FBI systems or data. Fingerprint based background checks must be conducted prior to initial hire and at least once every five years thereafter. Furthermore, if any agency employee has cause to enter the criminal justice system, or has improperly accessed or disseminated any CJIS or FBI data, all CJIS privileges shall be revoked and/or suspended and notification must be made to the CJIS Systems Officer (CSO) immediately. See FBI *CJIS Security Policy*.

3.16 Security – It is the agency head's responsibility to ensure that any area containing CJIS equipment, materials, and/or criminal justice information is physically secure from unauthorized use, viewing, or dissemination by all agency and contracted personnel. See the FBI *CJIS Security Policy* and the DCJIS CJIS Information Security Policies.

3.17 Timeliness - Appropriate and reasonable procedures must be in place to ensure that records in the CJIS and NCIC systems are entered, modified, and canceled in a timely manner to ensure maximum system effectiveness. See the CJIS Operating Manual and NCIC 2000 Operating Manual.

3.18 Training- It is the responsibility of the agency head to ensure that CJIS users are trained, tested, and certified within six (6) months of employment and every two (2) years thereafter.

3.19 Validation – Validation obliges the entering user agency to confirm that the record is complete, accurate, and still outstanding or active. See the NCIC 2000 Operating Manual.

3.20 Use of the System – ***Use of the CJIS including all applications, databases, equipment and services is for OFFICIAL CRIMINAL JUSTICE PURPOSES ONLY IN THE PERFORMANCE OF CRIMINAL JUSTICE DUTIES AS DEFINED BY APPLICABLE STATE AND FEDERAL LAWS.***

CJIS User Agreement – Acknowledgement

Type or Print Agency Name: _____ Date: _____

As a terminal agency utilizing the CJIS and NCIC systems, we hereby certify that we have read the User Agreement and acknowledge the duties and responsibilities as outlined in this document, as well as those documents incorporated by reference. We acknowledge that these duties and responsibilities have been developed and approved by the DCJIS in order to ensure the security, reliability, confidentiality, completeness and accuracy of all records contained in, or obtained by means of the CJIS and NCIC systems. We further acknowledge that failure to comply with these duties and responsibilities will subject this agency to various sanctions as approved by the DCJIS. These sanctions may include the termination of CJIS services.

List the ORI and the Agency code for all terminals covered by this User Agreement

	ORI # (ex: MA0010100)	**Agency Code** (ex: CAM)
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

List the type and quantity of mobile devices used by your agency covered by this User Agreement and any agencies in which a MOU may be applicable. (Include additional pages if necessary):

Agency Name	**Type**	**Quantity**
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Agency Head:

_____
Signature

_____
(Type or Print Name and Title)

_____
e-mail address

By signing above, I acknowledge that I have read and acknowledge that I have read and understand Appendix B

CJIS Representative:

_____
Signature

_____
(Type or Print Name and Title)

_____
e-mail address

By signing above, I understand the job duties described in the job duties described in Appendix C

Backup CJIS Representative:

_____
Signature

_____
(Type or Print Name and Title)

_____
e-mail address

By signing above, I acknowledge that I have read and acknowledge that I have read and understand Appendix B

CJIS Technical/Security Contact:

_____
Signature

_____
(Type or Print Name and Title)

_____
e-mail address

By signing above, I understand the job duties described in the job duties described in Appendix C

*Please only fax **pages eight (8) and nine (9) of this document** to 617.884.4601 or mail to CSS Unit of DCJIS*

- Attach and review for accuracy a TQ for each ORI used by your Agency.
    - This includes the ORI's assigned to CJIS Web and RMS/CAD systems. For Agencies with Open Fox terminals, attach/review a QO for each ORI as well

AGENCY STREETADDRESS_____

CITY, ZIP CODE_____

PHONE AND FAX#_____

Definitions

Advanced Authentication – Additional security functionality, in advance of the typical user identification and authentication, such as virtual private networks, biometric system, public key infrastructure, smart cards and token based devices.

Agency – Any housing agency of the federal, state or local government or a political subdivision, administering a subsidized housing program, or an organization under contract with such a public agency to administer a subsidized housing program.

Asymmetric Encryption – is the same as public-key cryptography, i.e., a form of cryptography in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key, and the receiver decrypts them using the private key. Using this method, the private key never has to be revealed to anyone other than the user.

CJIS Representative - The point of contact between the CJIS Support Services (CSS) unit and the CJIS user agency. Please see section (4.2) for a detailed list of administrative responsibilities to be executed by the CJIS Representative.

CJIS Systems Agency (CSA) - A CJIS Systems Agency (CSA) is a criminal justice agency which has overall responsibility for the administration and usage of the FBI CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories. There will be no more than one CJIS Systems Agency per state, district, territory, or foreign country.

CJIS Systems Officer (CSO) - A CJIS Systems Officer for each CJIS Systems Agency shall be appointed by the head of their respective agency. The CSO and his/her agency will be responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division.

Encryption – The process of obscuring information to make it unreadable without special knowledge in order to protect data from unauthorized individuals.

Hit - A record(s) obtained through a CJIS workstation in response to an NCIC or CJIS inquiry.

International Justice and Public Safety Network (Nlets) - An international, computer-based message switching system that links together state, local, and federal law enforcement and criminal justice agencies for the purpose of information exchange.

Interstate Identification Index System (III) - The cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National

Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

Local Housing Authority (LHA) – A local housing authority or regional housing authority which was created pursuant to M.G.L. c. 121B and operates there under, including Housing and Community Development (HCD) or its designated agent, to the extent that HCD is acting as a local housing authority pursuant to M.G.L. c. 121B, § 26A.

Management Control - Each CJIS workstation must be under the management control of a criminal justice agency.

Management control is defined as the authority to set and enforce:

(1) Priorities;
(2) Standards for the selection, supervision, and termination of personnel;
(3) Policy governing the operation of the CJIS workstation; and
(4) Policy regarding the physical security of the workstation as well as the building housing said workstation.

Memorandum of Understanding (MOU) - An agreement between any terminal agency and other criminal justice agency that details the scope of the services to be provided to the non- terminal agency and specifies each agency's responsibilities as they pertain to all services provided. (i.e. the entering of a missing person record into the CJIS and NCIC Networks by a terminal agency for a non – terminal agency.) Please see section (4.4) for the administrative responsibilities regarding MOU's.

National Crime Information Center (NCIC) - The computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the Attorney General of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information. The NCIC includes, but is not limited to, information in the III System.

National Fingerprint File (NFF) - A database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

Non-Secure Location - A criminal justice facility, an area, a room, a group of rooms, or a police vehicle that does not satisfy the criteria of a physically secure location.

Non-Terminal Agency - Any criminal justice agency which does not have direct access to the NCIC and CJIS networks. These agencies must execute a Memorandum of Understanding (MOU) with a terminal agency in order to ensure that important criminal justice data is entered, modified, and cancelled in the NCIC and CJIS systems. See (3.11) for more details.

Non-Twenty-Four Hour Criminal Justice Agency - Any criminal justice agency which has a CJIS workstation that enables a user to enter, modify and cancel records, but which may not have staff available twenty-four hours a day to respond to hit confirmation requests as required by NCIC standards.

Physically Secure Location - A criminal justice facility, an area, a room, a group of rooms, or a police vehicle that is/are subject to criminal justice agency management control/security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS network. Physical security perimeters shall be defined by the CSO. Law enforcement sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access. Every physical access point to sensitive facilities or restricted areas housing information systems that access, process, or display CJIS data shall be controlled/secured in a manner which is acceptable to the CSO during both working and non-working hours.

Primary Entry CJIS Workstation – A CJIS workstation located within a user agency that has entry capabilities twenty-four (24) hours a day, seven (7) days a week and is used to enter, modify or cancel a record. Those agencies that do not have entry capabilities twenty-four (24) hours a day, seven (7) days a week should have a MOU with a user agency possessing those entering capabilities.

Record - Criminal justice data entered into CJIS and NCIC through a CJIS workstation regarding missing persons, wanted persons, and stolen property is contained in an electronic file with a unique reference number. This file may be “pulled” at a later time to modify or cancel depending upon whether different information is obtained or the person or property is located.

Regional Working Groups (RWG) - A geographic separation of the Massachusetts CJIS user community by region (seven regions in total) in order to more easily conduct meetings in which CJIS application and network updates are given, trainings may be provided and discussion for system improvement is encouraged.

Related Agency Doctrine – A legal principle providing for the re-dissemination of FBI criminal history record information (CHRI) by an authorized recipient. Agencies that have commonality of purpose and (typically) congruent responsibility, authorized by federal statute or executive order, or state statute approved by the Attorney General of the United States pursuant to Public Law 92-544 can receive FBI CHRI and exchange information with each other for the authorized purpose originally requested.

Terminal Agency - Any criminal justice agency which has direct access to the NCIC and CJIS networks through a CJIS workstation that enables a user to enter, modify, and cancel records containing important criminal justice data.

Symmetric Cryptography – Messages are sent and received using the same key for encryption and decryption.

Virtual Private Networks (VPNs) - VPNs use security mechanisms to effectively create a private network across a shared (usually public) communications backbone connecting distributed elements or members of a single organization. The interconnecting communications backbone may consist of leased lines, dial-up service, packet and cell switched connection-oriented networks, and/or routed connectionless networks. VPNs are also

useful in restricting distribution among subsets of the organization at large.

Typically VPNs may be utilized to securely communicate between:

(a) Site-to-site infrastructure across a public communications backbone.
(b) Local Area Network (LAN)-to-LAN subnets operating across a network that services other entities outside the VPN community.
(c) Host-to-host workstations across a shared network or subnet.

Appendix B
CJIS User Agency Head Description of Responsibilities

The Department of Criminal Justice Information Services (DCJIS) requires that each Agency Head ensure the policies and procedures of the Massachusetts Criminal Justice Information System (CJIS) and National Crime Information Center (NCIC) Systems are upheld and the efficiency of the aforementioned systems is maintained within his or her jurisdiction. This may be accomplished through the monitoring and assurance of proper use of the CJIS/NCIC network in addition to appointing qualified and experienced professionals as the CJIS Representative, backup Representative and CJIS Technical Contact(s).

Listed below are the responsibilities of the Agency Head:

- Must develop formal written procedures regarding the operational use and security of CJIS to ensure compliance with CJIS and NCIC policy and regulations. Compliance will be measured by CJIS Support Services (CSS) Unit audits which will occur once every two years via a mail survey or an in-person interview.

- Ensure that all equipment connected to the CJIS Network has been approved by the DCJIS. In addition, the agency head shall be responsible for sustaining a maintenance agreement with a DCJIS approved vendor for each router, and switch the agency possesses.

- If any problems should occur with the above referenced CJIS equipment, you must contact the Executive Office of Technology Services and Security (EOTSS) immediately at (617) 660-4620.

- Ensure that pre-employment background screening is conducted on all personnel who have authorized access to CJIS and FBI systems and data ,and, further, that fingerprint based background checks are conducted on all personnel; at least once every five years. In addition, if any individual or administrator who accesses or uses CJIS and/or FBI data is convicted of a misdemeanor or felony the Agency Head must immediately notify the Commonwealth's CJIS Systems Officer in writing of the circumstances. Access for any individual who is convicted of a felony must be suspended immediately. Access for any individual convicted of a misdemeanor must be suspended until the CJIS systems officer makes a determination as to whether or not access should be reinstated. Any individual that improperly accesses or disseminates data or information from any CJIS or FBI system shall have their access privileges suspended or terminated. Continue to uphold that the CJIS/NCIC system should only be utilized for criminal justice purposes only. Use of the CJIS/NCIC systems, including the Registry of Motor Vehicles for non criminal justice purposes, including transactions conducted for public and private educational establishments, municipal agencies, town government officials, etc. is strictly prohibited and is punishable by a fine, suspension of services and/or incarceration.

- Maintain that any area containing CJIS equipment, materials, and/or criminal justice information is physically secure from unauthorized use, viewing, or dissemination by all non- authorized agency and contracted personnel. See the FBI *CJIS Security Policy* and the DCIJS CJIS Information Security Policies.

- Ensure that CJIS Users are trained, tested, and certified within six (6) months of employment and every two (2) years thereafter.

Appendix C

Criminal Justice Information System Representative Description of Responsibilities

The Department of Criminal Justice Information Services (DCJIS) requires that each Agency Head ensure that the individuals he or she appoints as a CJIS Representative, backup Representative and Technical Contact possess the qualifications and knowledge necessary to act as a liaison between the CJIS department and your agency. This is to ensure the policies and procedures of the Massachusetts Criminal Justice Information System (CJIS) and National Crime Information Center (NCIC) Systems are upheld and the efficiency of the aforementioned systems is maintained.

According to the requirements stated in the CJIS User Agreement, listed below are the responsibilities of the CJIS Representative and backup Representative:

- Ensure that training is available to all authorized CJIS users within six (6) months of employment and every two (2) years thereafter. Authorized CJIS users can be defined as individuals who require direct access to CJIS/NCIC systems to perform criminal justice related functions.

- After the completion of the required training each user must take the CJIS Policy and Security Awareness Test located on the nexTEST online CJIS exam website.

- Provide certificates of achievement for the successful completion of training and a passing score of seventy (70) or above on the appropriate examination.

- Ensure that the validation process is completed and submitted to the CJIS Support Services (CSS) Unit on or before each month’s specified due date.

- Proper password maintenance as required by CJIS security policy, including the disabling of accounts for individuals who have been suspended, fired, retired, or have voluntarily terminated their own employment.

- Attendance at the biannual Regional Working Group meeting. If neither the CJIS Representative nor his/her backup are able to attend, the agency head may designate another agency employee to be present.

- Timely responses to communications from the DCJIS.

- Distribution of publications to agency personnel as directed by the DCJIS.

Appendix D

Criminal Justice Information System Technical / Security Contact Description of Responsibilities

The Department of Criminal Justice Information Services (DCJIS) requires that each Agency Head ensure that the individuals he or she appoints as a CJIS Representative, backup Representative and Technical Contact possess the qualifications and knowledge necessary to act as a liaison between the CJIS department and your agency. This is to ensure the policies and procedures of the Massachusetts Criminal Justice Information System (CJIS) and National Crime Information Center (NCIC) Systems are upheld and the efficiency of the aforementioned systems is maintained.

According to the requirements stated in the CJIS User Agreement, listed below are the responsibilities of the CJIS Technical Contact(s):

- The CJIS Technical/Security Contact(s) is responsible to ensure the proper technical/security administration of the CJIS at the local level.

- Ensure that due to the highly sensitive nature of the CJIS Network, no individual shall touch, replace, hinder or reconnect any CJIS equipment without the consent of DCJIS. Furthermore, you are required to provide notification of any desired relocation, exchange, or replacement of a CJIS switch, router or any other CJIS related equipment in writing to CJIS Support Services (CSS) Unit a minimum of fifteen (15) business days prior to the planned relocation, exchange, or replacement.

- Make certain that all problems experienced by user agencies regarding the CJIS and all CJIS equipment shall be reported to the Executive Office of Technology Services and Security (EOTSS) directly at (617) 660-4620 for troubleshooting and further escalation if necessary.

- For any mobile/wireless devices accessing the CJIS network you must ensure that transaction logs are maintained for a minimum of two (2) years and are readily available at the request of DCJIS or any other agency head.

- In the event a security incident, which is a violation or a potential violation of the confidentiality, integrity and/or the availability of state/FBI CJIS data occurs, you must ensure that the Agency Head submit a fax, on agency letterhead, to the attention of the Department of Criminal Justice Information Services (DCJIS) Commissioner, CJIS Systems Officer to (617) 884-4601 within forty-eight (48) hours with the following information:
  - Date & location of incident
  - System affected
  - Method of detection & nature of incident
  - Description of the incident & actions taken/resolution
  - Date & contact information for the agency



1081

1 Antares Dr., Suite 400
Ottawa ON, K2E 8C4
Canada

i2 Product Quotation

Jul 15, 2022

Dear Elly Smith,

Thank you for your inquiry about i2 offerings.

All prices herein are suggested prices only and are subject to change at i2's sole discretion. Products listed herein are subject to withdrawal or modification by i2 at any time at i2's sole discretion. Final coverage dates for new license, Software Subscription and Support reinstatement, and Software Subscription and Support renewal part numbers will be based upon i2's acceptance of the order, and as specified in the applicable agreements, irrespective of the dates which may appear in this quote.

This quotation is valid from Jul 15, 2022 and will expire on Sep 30, 2022.

Your order will be governed by and is subject to the terms of the agreement, as applicable, against which this transaction will be placed.

Data Processing Protection – i2's Data Processing Addendum (DPA) and the DPA Exhibit at www.i2group.com/legal apply to Client personal data, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679); and ii) other data protection laws identified i2 data processing link apply.
If you need assistance with placing your order or wish to discuss your quote, please contact the i2 contact noted below.

Yours sincerely,
John Wintrow
Sales Reps
Phone Number:
E-mail Address: john.wintrow@i2group.com

Quotation Detail

Quote No:	i2 -15675
Effective Date:	Jul 15, 2022
Expiration Date:	Sep 30, 2022

Customer Details

Organization name:	COMMONWEALTH OF MASSACHUSETTS
Account number:	8128593
Attn Contact name:	Elly Smith
Attn Contact email:	eleanor.smith@state.ma.us
Billing Address	One Ashburton Place Boston US Massachusetts 01754-1227

Product Details

Item	Part #	Description	Quantity	List Price	Extended Price
1	D0PR8LL	i2 Analyst's Notebook Premium from i2 Analyst's Notebook Concurrent User Trade Up License	9	$144,000.00	$115,650.00
2	E0DQWLL	i2 Analyst's Notebook Premium Concurrent User Annual SW Subscription & Support 12 Months	9	$45,000.00	$45,000.00

Summary

Total	**$160,650.00**

Applicable tax will be calculated at the time of order processing. If tax exempt, please include your certificate with your order.

i2 acceptance of the order is subject to credit approval.

Data Processing Protection – i2's Data Processing Addendum (DPA) and the DPA Exhibit at www.i2group.com/legal apply to Client personal data, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679); and ii) other data protection laws identified www.i2group.com/legal apply.

N Harris (Canada)

Name:
Title:
Executed Date:

Signature:

COMMONWEALTH OF MASSACHUSETTS

Name:
Title:
Date:

Signature:

AIRSHIP

TAILORED. VIDEO. INTELLIGENCE.

EMS

SYSTEM ADMINISTRATOR

QUICK REFERENCE GUIDE

CONTENTS

ABOUT THIS MANUAL **4**
Version Requirements 4
Version Updates 4
COPYRIGHT AND DISCLAIMER **5**
Copyright 5
Disclaimer 5
OVERVIEW **6**
New Features *6*
Log In to EMS *6*
Dashboard 6
Quick Actions *7*
Event Log *7*
Recently Active Users *7*
Menu Options 7
USERS **8**
Users List 8
Create a New User 9
Edit a User 10
User Groups 11
IP Cameras 12
IP Camera List 12
Assigning Cameras to a Case *12*
Add an IP Device 13
Additional Options 14
Audio/Video Settings 15
CASES **16**
Export Disk Usage Reports *17*
Transitioning a Case *18*
Deleting Case Footage *18*
AUXILIARY DEVICES **19**
LOCATIONS AND TAGS **20**
Tags 20
Locations 20
Locations Example *21*
VIDEO IMPORTS **21**
EVENTS **21**
ABOUT **22**
Contact Info *22*
License Info *22*
Usage Report *22*

©2021 Airship Industries

Database Information *22*

SYSTEM ADMINISTRATOR ADVANCED OPTIONS 23

Adding System Components 23

Transcoders 23

Archivers 24

Add Archiver to EMS: *24*

Archiving Video *24*

VSHs 25

Failover Options *26*

Analytic Engines 26

Windows Credentials 27

Software Update 27

System Versions *27*

Add Software Installers *28*

Settings 29

General *29*

LDAP Settings *31*

Mail Server *32*

Permission Levels 33

Custom Permissions *33*

GLOSSARY 34

NOTES 35

ABOUT THIS MANUAL

This document assumes that the reader has familiarity not only with the majority of the **Airship** software products but also with computer networks and operating procedures.

Further, this document assumes that the reader has previously installed a functional **EMS** and is an administrator on that **EMS** (with authority to make changes to that system and the network).

Version Requirements

As of this manual's publication, the following versions are available for **EMS**, **Airship Server** and **Nexus**:

- EMS 7.2.0
- Airship Server 7.2.0
- Nexus Client 7.2.0

Version Updates

- UI Redesign
- Improve timezone support for all assets
- Added additional columns for Operating System, Serial Number information for VMS assets
- Added ability to edit NVR type VMS assets (Managed Setup Tool)
- NVP export process are now logged as events in EMS
- Added licensing features for EDS portal
- Disable option to enable SMS 2FA if Twilio service is not configured
- Hide Login with Windows button if SSO is not configured
- Update required Java runtime from Java8 to Java11

©2021 Airship Industries

COPYRIGHT AND DISCLAIMER

Copyright

This publication, including all photographs, illustrations, instructions, and software, is the property of **Airship** Industries, Inc. The copyrights and intellectual property rights associated with this publication and its contents are protected by international copyright laws, with all rights reserved. Neither this manual nor any of the material contained herein, may be rewritten, reproduced or shown to the public without first receiving the written consent of **Airship**.

Disclaimer

The information in this document has been prepared by **Airship**'s current system policies and procedures and is subject to change without notice. **Airship** reserves the right to revise or amend this publication and make changes periodically, without any obligation to notify any person of such amendments or revisions.

Airship makes no representations or warranties that the hardware will work properly in all environments and applications, and specifically disclaims any implied or express warranties with regard to the quality, performance, merchantability, or fitness for a particular purpose.

In no event shall the copyright owner or contributors to this manual be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including but not limited to procurement of substitute goods or services, loss of use, data, or profits, or business opportunity), however caused and arising out of any theory of recovery, arising out of the use of this software.

OVERVIEW

The **Enterprise Management System (EMS)** is a centralized management server that is used to map a set of **Airship Servers** and **Nexus Clients** into a central database for easy administration.

This manual outlines all the available options within EMS to a System Administrator. This includes creating Users, User Groups, custom Permission Levels for users, adding IP Cameras and other devices all through a web interface that is accessible from anywhere on the LAN.

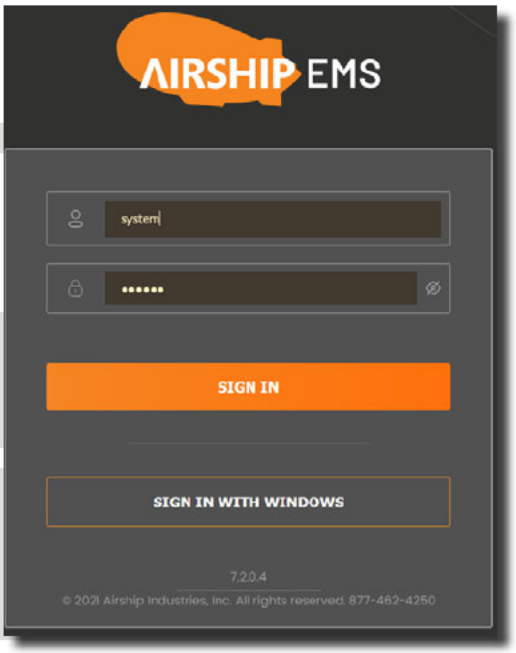
This manual loosely follows standard workflow procedures dictated by navigating down through menu options.

New Features

In the interest of improving ease-of-use, users upgrading from a prior version of **EMS** will notice the new wizard-style interface. Most workflow remains the same and any differences are covered within this manual.

Log In to EMS

Begin by accessing **EMS**. Open a web browser (Chrome or Firefox), and use the IP (or "localhost") and port followed by "/ems" as in the example below. The default port for **EMS** is 8080.



> ***EXAMPLE***: 127.0.0.1:8080/ems OR localhost:8080/ems

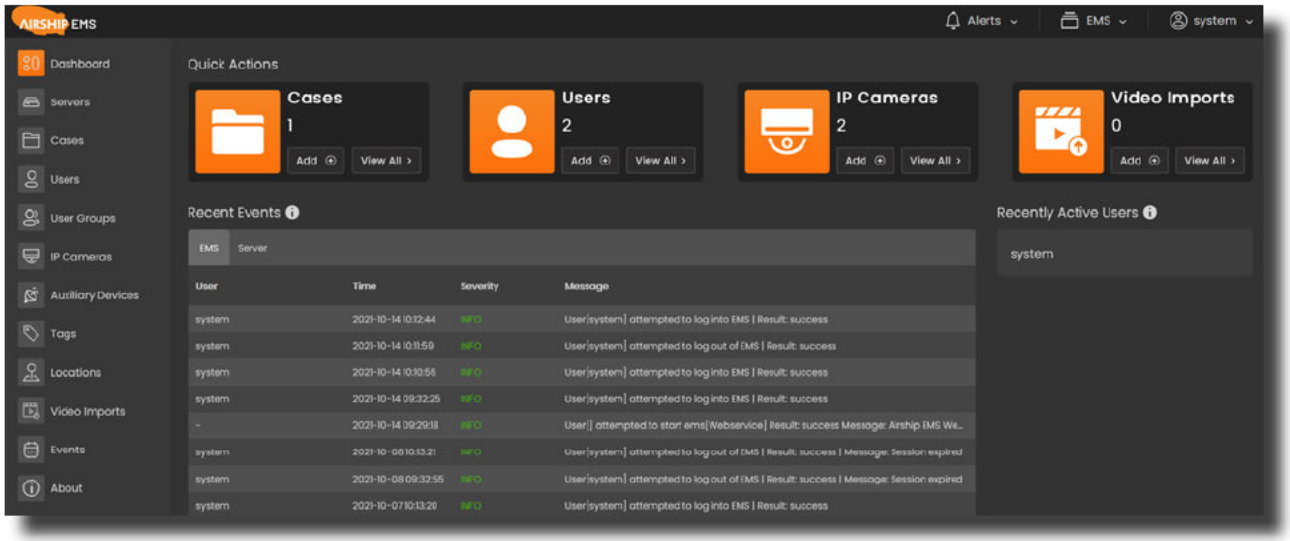
The default username is “system”, and the password is “system”. Click **Submit** to log in to the **EMS**.

> **IMPORTANT:** To use Windows credentials to log in to **EMS**, click the "Sign In with Windows" button. This feature is called Single Sign-On(SSO), and requires some setup before it can be used. For information on setup, see **Airship’s *‘SSO Quick Reference Guide’***.

> **NOTE**: Once logged in, if there are sections missing from your version of **EMS**, it is likely the proper license has not been imported. Call **Airship** Support to properly license **EMS**, or if you have a license already generated by Airship, upload into EMS by going to **About** > **License Info** and click **Add License**.

Dashboard

Access the most common action items in **EMS** by visiting the system’s Dashboard as shown in the screenshot below. To return to the Dashboard from any page in **EMS**, click Dashboard at the upper left.



©2021 Airship Industries

Quick Actions

The most common actions are located on the main dashboard for quick access. Users can add or view all cases, users, or IP cameras by clicking the links near the top of the dashboard.

Cases: Displays the number of cases created. See "Cases" on page 16.

Users: Lists the current number of Users created. See "Users" on page 8.

IP Cameras: Displays the number of Cameras connected to **EMS**. See "IP Cameras" on page 12.

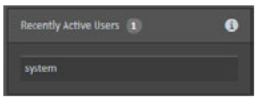
Video Imports: Lists the number of Videos imported. See "Video Imports" on page 21.

Event Log

Below Quick Actions, an Event Log displays the most recent events triggered with **EMS**, **Failover**, or **Airship Server**.

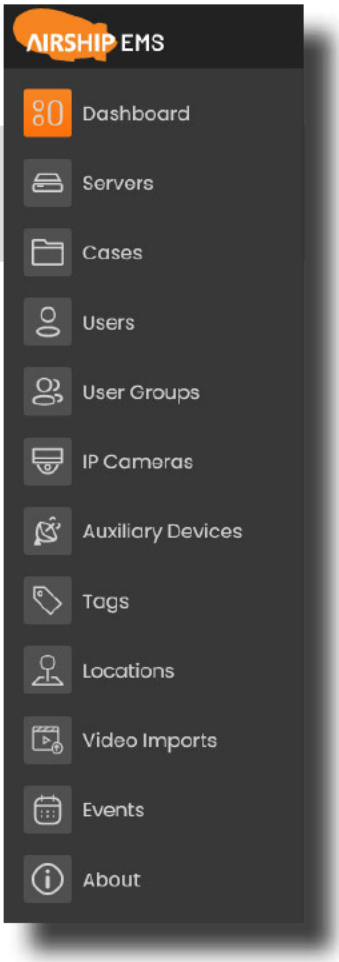
Recently Active Users

Lists users that have logged in at least once within the past three (3) days.



Menu Options

After logging in, the **EMS** has a list of menu options under **Dashboard**. Most capabilities of **EMS** are accessible with only a click or two from the left-hand navigation menu (pictured on right).



📖 **NOTE:** Administrators have additional access to advanced features by clicking the username located at the top right of the EMS window and selecting "Advanced". See "System Administrator Advanced Options" on page 23 for more information.

USERS

Users logged into **EMS** have varied levels of access depending on the User Group assigned to their username. A ***System Administrator*** may create new users and assign user groups.

- Every user created must belong to at least one user group or they may belong to multiple groups.
- Users can be assigned to the built-in user groups or you can create a new user group and assign users.

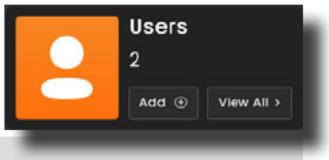
The built-in User Groups levels are as follows:

- **System Administrators** are able to make system-wide changes such as create users, IP devices, locations, tags, and more, which they can assign to power users and operators. Admins have access to additional advanced features in **EMS** (covered in "System Administrator Advanced Options" on page 23).
- **Power Users** are able to make some changes within **EMS** to the location to which they are assigned, such as create users and other assets.
- **Operators** (end-users) only use **Nexus** or **Video Portal** to view the cases, servers and the cameras to which they have access. These users do not have access to making changes within **EMS**.

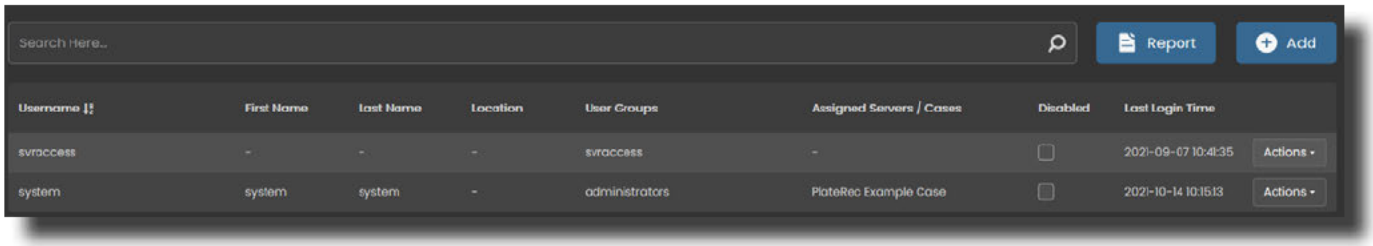
Further custom Permission Levels may be assigned per group and managed by the ***System Administrator***.

Users List

To access the list of users, either click **View All** from under the "Users" frame (pictured) located on the **Dashboard**, or click **Users** from the left-hand navigational menu. From this page, System Administrators may add, edit and delete users.



📖 **HELPFUL HINTS:** Click any one of the column headings to sort the order of the User's list.



Username: Displays the login name of the user.

First Name: Displays the first name of the user.

Last Name: Displays the last name of the user.

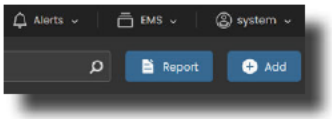
Location: Displays the user's system-related location.

Disabled: Check this box to disable the user.

Actions:

- **Edit:** Click to modify the user information.
- **Delete:** Click to remove a user from the list. User will be prompted to confirm before deleting.

A full list of users can be generated by clicking the **Report** button in the top right corner.



A drop-down menu appears to either Export a list of users as a .csv file or View the Report of the selected users.

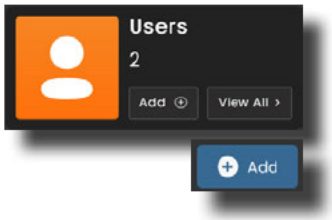


©2021 Airship Industries

Create a New User

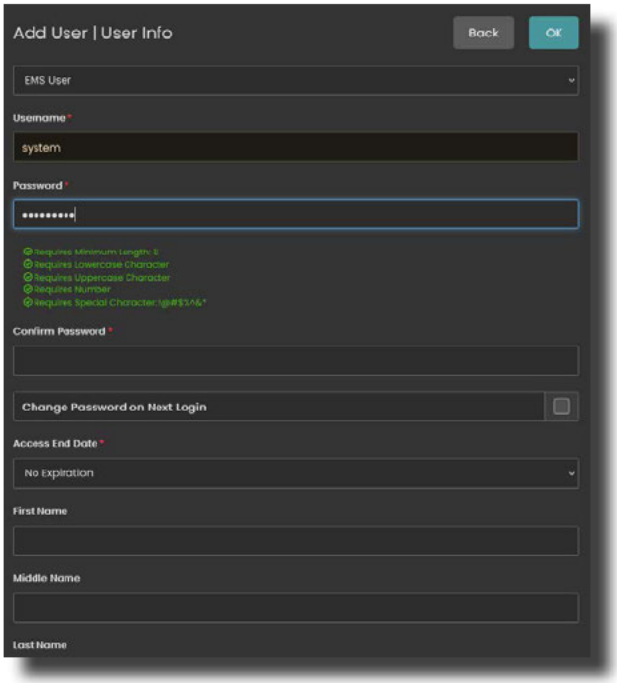
Adding a user is as simple as creating a username/password and assiging a User Group to the new user. Additional fields may provide further detail if desired.

1. Click "Users" from the left-hand navigational menu; or click "Add" from the Dashboard located under the orange "Users" frame (pictured) and skip to step 3.



2. Click "Add" from the Users list.
3. Click "User Info".
4. With the "Add User | User Info" page open, enter or select the appropriate information.

📖 **IMPORTANT**: All the boxes with a red asterisk (*) are mandatory.



***Username:** Enter a login name for the user.

***Password:** Enter the password for the user to login.

📖 Password requires eight characters at a minimum, and at least one number, uppercase, lowercase, and a special character.

***Confirm Password:** Enter the password again to confirm it.

***Change Password on Next Log In:** Check this box to prompt the user to change their password upon their next login. User cannot log in to **EMS** until the password is changed.

***Access End Date:** By default, there is no expiration, to set a date for disabling the user, select a timeframe from the drop-down, or enter a custom range.

First, Middle, Last Name: Enter the name of the user in each field (not required).

Location: Select a location from the list to add the user to a location.

📖 **HELPFUL HINTS:** When a Power User adds a new user, the Location list shows only that location to which the Power User belongs.

Description: If desired, a description of the user may be entered for future reference.

Service User: Service users are exempt from auto-lockout after login failures, expiration dates, and are not forced to reset their password if it surpasses the password age limit set. Check this box to set the user as a Service User.

Receive Email Notifications: Check this box for the selected user to receive notification of alarm events.

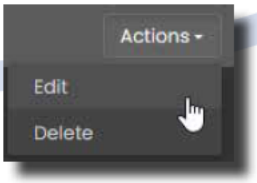
📖 **NOTE**: Set the email address for the User in the "Contact Details" section. Nexus Mobile notifications may be set via the App.

5. When details have been entered, choose **OK** or **Back** to advance.
6. Next, assign a User Group by clicking one of the available options and click **OK**. For adding new groups, please read the steps required found in the section below, User Groups.

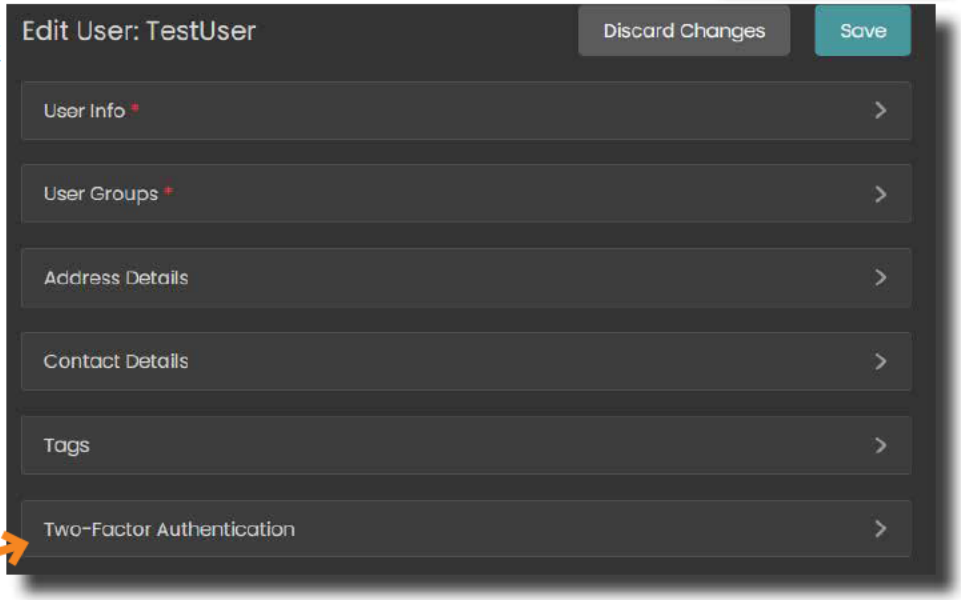
Edit a User

To edit an existing user:

1. From the Users List, select which user to edit.
2. In the **Actions** column, click **Edit** from the drop-down to open the **Edit User** page (similar to the **Add User** page).



3. Choose to edit User Info, User Groups, Address Details, Contact Details, Tags, or enable Two-Factor authentication for the selected user.



📖 **Two-Factor Authentication**: To enable Two-factor Authentication, set the Two-Factor Authentication Type in the Advanced Settings menu under General. After setup and upon next login, the user will be required to verify two-factor authentication with either a QR code reader app (such as Google Authenticator) and a 6-digit code, by Email only, or by Email and SMS. Non-admin Users may turn on/off 2FA, but only for their own account.



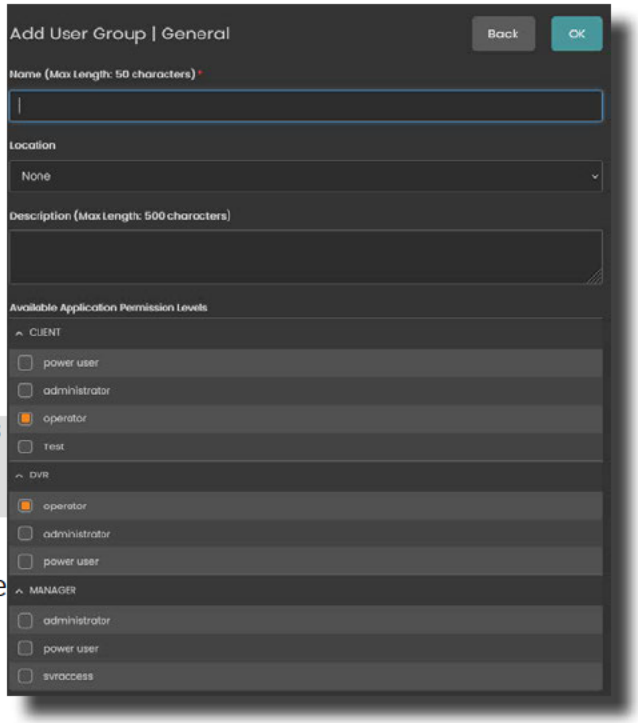
📖 **NOTE**: Adding users with LDAP authentication will require the System Administrator to navigate to "System Administrator Advanced Options" on page 23.

©2021 Airship Industries

User Groups

User Groups determine the level of access outlined above in the "Users" on page 8.

1. User Groups may be added by either clicking "User Groups", then "New Group" or click "New Group" while adding a new user.
2. While creating a New User Group, an admin selects the desired permission levels to applications such as Client (**Nexus**), DVR (**Server**), Manager (**EMS**) and then assigns the permission level per application.



📖 Further information regarding how to assign permissions is covered in the ***Airship Permission Levels Quick Reference Guide.***

3. Once a User Group is created, System Administrators may assign users to it by clicking the **Users** tab while editing the new Group.

4. To assign the User to the User Group, check the box next to the username, then click **OK**.
5. Click **Save**.



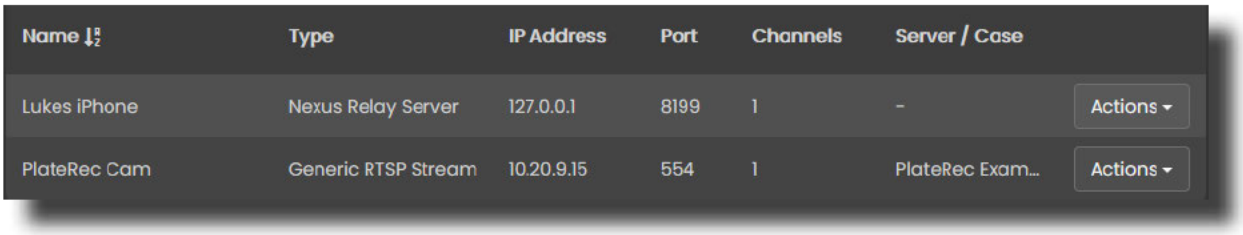
IP CAMERAS

Users can add IP cameras to **EMS** in three different ways. You can add a single IP device, add devices from a file, or add from an IP address range.

IP Camera List

Select **IP Camera** from the list to see all the IP cameras on **EMS**.

📖 **HELPFUL TIP:** Click any one of the column headings to change the order of the 'IP Camera List' in ascending or descending order.



The section below explains all the columns in the 'IP Cameras List'.

Name: Displays the name of the camera/device.

Type: Displays the manufacturer name of the camera.

IP Address: Displays the IP address of the camera/device.

Port: Displays the port number on the camera/device used to deliver video.

Channels: Displays the number of channels utilized by the camera/device.

Server/Case: Displays the case or server which the device is assigned.

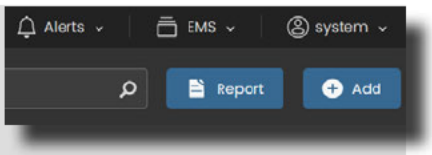
Actions: ***Edit:*** Click this button to modify the camera information.

***Delete*:** Selecting this option will remove the camera/device. You will be prompted to confirm before deleting.

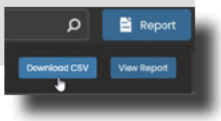
Assigning Cameras to a Case

IP cameras and other devices may be assigned to cases on VSHs. To assign a camera to case, see "Cases" on page 16.

📖 A full list of IP devices can be generated by clicking the **Report** button in the top right corner.



A new page will populate the list of IP devices, which can be exported as a .csv file by clicking "Export CSV" in the top right corner of the Report page.

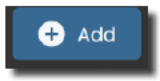


©2021 Airship Industries

Add an IP Device

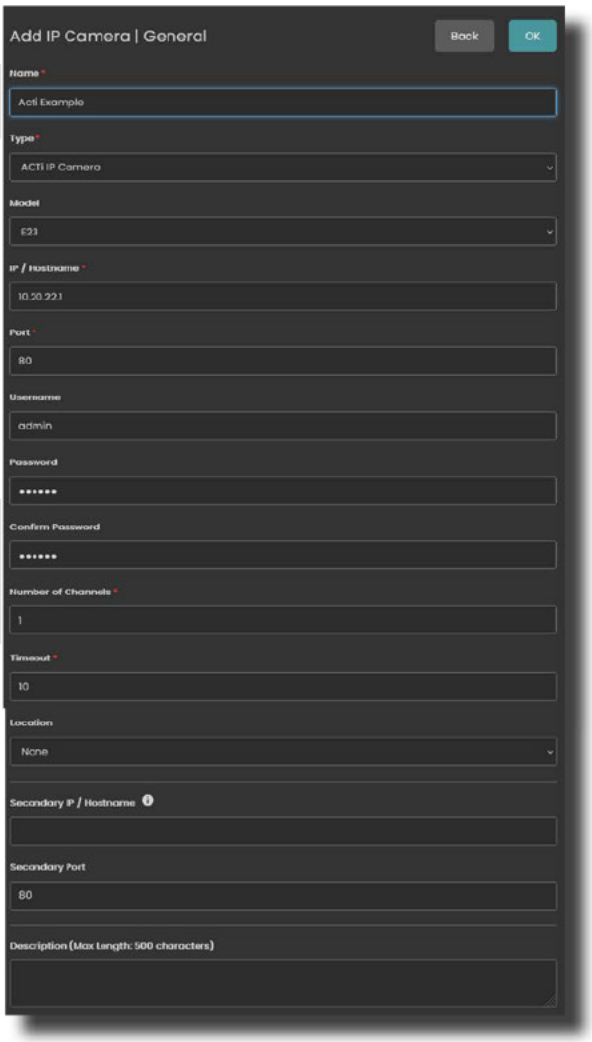
To add a new IP Device such as a camera or an encoder:

1. Click **IP Cameras** from the left-hand navigational menu, and click the **Add** (+) button.



2. The **Add IP Camera** page opens. Enter or select the appropriate information:

📖 All the boxes with a red asterisk (*) are mandatory.



***Name:** Enter the name of the camera.

📖 Input camera names per standard naming convention.

***Type:** Select the camera type from the list of manufacturers supported by **Airship**.

Model: Based on the Type of camera, select the Model from the drop-down list (not required).

***IP/Hostname:** Enter the IP address of the camera.

***Port:** Enter the port number of the camera.

📖 Port information can be found on the web-based camera interface or in the camera manufacturer's documentation.

Username: Enter the camera's username to access the camera (most, but not all cameras require a username/ password).

Password: Enter the camera's password to access the camera.

***Number of Channels:** Default is 1. If this IP device has more than one channel, ensure that the exact number of channels is entered; it cannot be changed after saving.

***Device Timeout:** Enter the value for time out; After the specified value of timeout, the server will stop connecting to the camera. Default is 10 seconds.

Location: Select a location from the list to add it to the IP camera.

📖 When a power user adds a new IP camera, the Locations list only shows the location to which the power user belongs.

Secondary IP & Port If the camera being added shares a secondary network & port, enter it here.

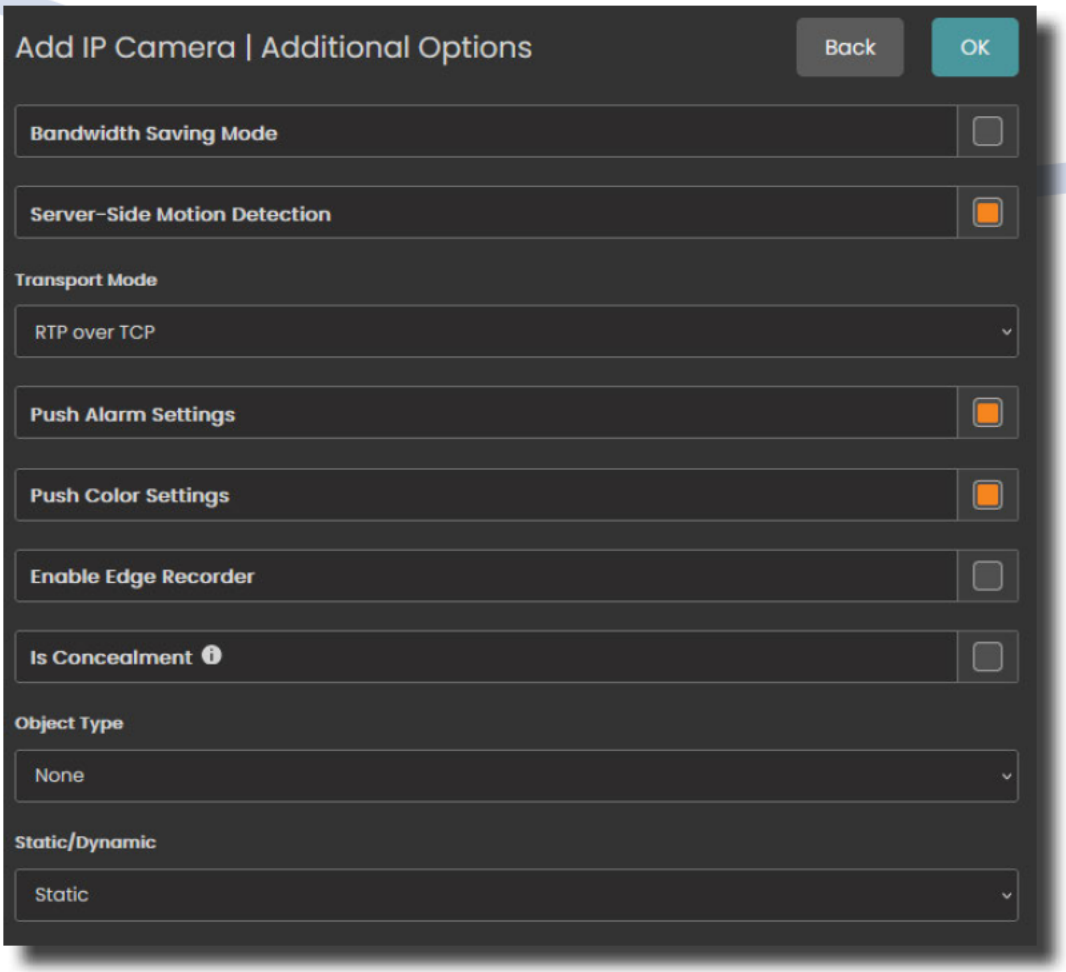
Alarm Inputs: Enter the number of 12v or RS-485 alarm inputs.

Alarm Outputs: Enter the number of 12v or RS-485 alarm outputs.

Description: Enter a short description of the camera.

3. Additional (optional) information and associations may be filled out by clicking through each section. Click Additional Options, Audio/Video Settings, Permission Levels, Tags or Auxiliary Devices to configure the IP device further.

Additional Options



Bandwidth Saving Mode: When enabled, the assigned VSH only connects to the camera when motion is detected by the camera or when Live View is requested by a client. The video stream disconnects when motion expires, and live view is disconnected.

Server-Side Motion Detection: Check this box to enable server-side motion detection, which measures changes in color each frame to determine if motion occurs. This feature is designed for use when no camera-side motion detection is supported at the cost of significantly higher CPU utilization.

Transport Mode: Select the streaming protocol used by the camera.

Push Alarm Settings: Check this box to enable EMS to push alarm settings to the camera.

Push Color Settings: Check this box to enable EMS to push color settings to the camera.

Enable Edge Recorder: When streaming bandwidth is limited, check this box to store footage directly at the device (Edge) and retrieve selected footage on demand.

Is Concealment: Check to mark this IP device as a concealment for search purposes.

Object Type: Select to associate an icon with the object type when displayed on map features in Nexus Client.

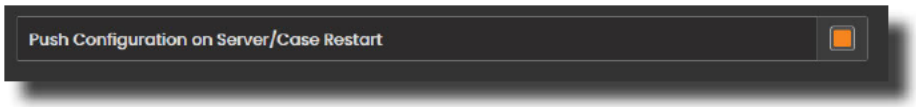
Static/Dynamic: Select the IP Address as Static or Dynamic depending on your network.

©2021 Airship Industries

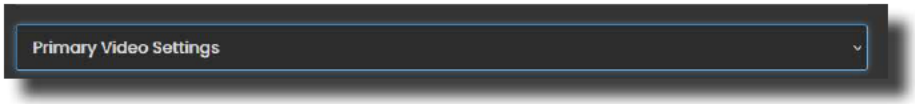
Audio/Video Settings

Audio and Video configuration options vary and are presented based upon the model device/camera added to **EMS**.

Push Configuration on Server/Case Restart: Settings made from this page can be pushed to the camera by selecting this box. These settings are pushed upon Server/Case restart.



Configure Components: Select from the drop-down menu, which first selects "Primary Video Settings" in order to edit audio and video components native to the camera.

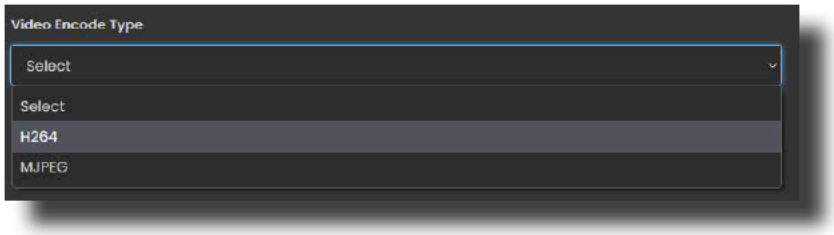


Each audio/video profile may be configured independently using this drop down menu.

Primary: The primary stream is what is recorded to disk by Airship Server. Select Primary for this camera in order to automatically stream the Primary video profile settings when the video is in focus.

Secondary: Select Secondary stream when trying to optimize viewing many video screens at once in Nexus Client.

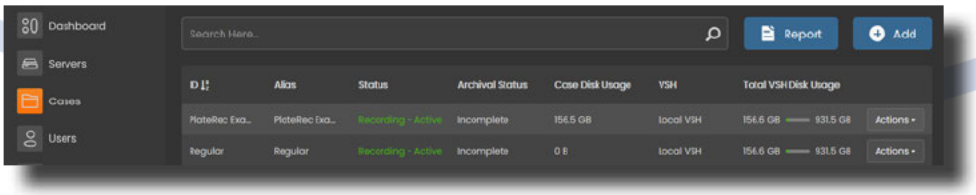
Video Encode Type: Select the type of encoding performed on the streaming video. Options presented are based upon the features available model of the device.



CASES

Cases allow for individulized access to defined groupings of cameras and custom permission levels.

1. To begin setup, click **Cases** from the left-hand navigational menu.



🕮 The section below explains all the columns in the 'Case List'. To add a Virtual Server Host, see "VSHs" on page 25 below. Click any column to sort alphabetically.

ID: Displays the case ID. (example: ME123)

Alias: Displays the case alias of the case. (example: Main Entry Buidling 123)

VSH: Displays the VSH name to which the case is assigned.

Status: Displays the current status of the case. Click **Transition** in the **Actions** column to change the case status.

Archival Status: ***Incomplete:*** The archival operation has not been performed. Refer to "Transitioning a Case" on page 18 for more information.

🕮 **NOTE:** Archival operation can be done on cases whose state is either Playback-Active or Deactivated.

Complete: The archival operation is complete. Users can close a case only when its archival process is complete.

Disk Usage: Displays the current amount of space taken up by the case in the destination folder.

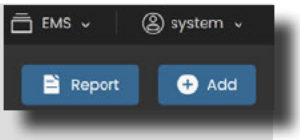
Total VSH Disk Usage: Displays the current total amount of space used by the VSH.

Actions: **Edit:** Select this option to modify the case information. You can edit only Recording-Active or Playback-Active cases.

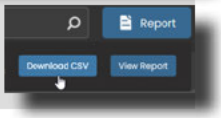
Restart: Select this option to restart a case. This option only works when in Recording-Active or Playback-Active.

Transition: Select this option to change the case status. Refer to "Transitioning a Case" on page 18 for more information.

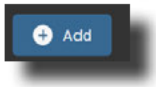
🕮 A full list of cases can be generated by clicking the **Report** button in the top right corner.



Select to Download the report as a .csv file, or View the Report from a web page.



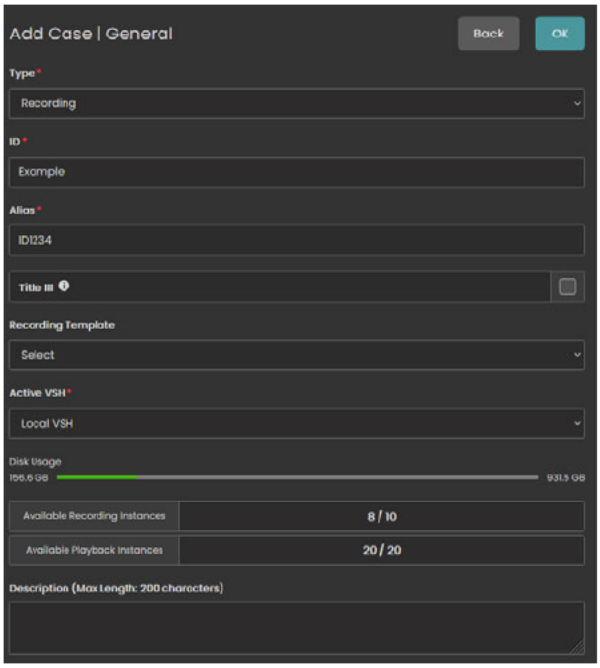
2. Click **Add** in the top-right corner, then begin setting up the case by clicking **General**.



©2021 Airship Industries

3. Enter all necessary information.

📖 All boxes marked with a red asterisk (*) are mandatory.



***Case Type:**	Select Recording, Playback from Airship Archive, or Playback from Nexus Archive.
***ID:**	Enter a unique case ID such as "ME123"; IDs cannot be the same.
***Alias:**	Enter an alias for the case, such as "Main Entry Building 123".
Title III:	If enabled, all recordings on the case must be toggled manually to record from Nexus Client. After enabling, the option to always record will be presented.
Recording Template:	Click the drop-down menu to select from Motion, Recording 24-7, No Recording, or 24-7 Constant and Motion Recording.
***Active VSH:**	Click the **VSH** for which to assign the case.
Disk Usage:	Displays the space used and available for the selected **VSH**.
Available Recording Instances:	Displays the currently available Instances licensed for the selected **VSH**.
Available Playback Instances:	Displays the currently available Instances licensed for the selected **VSH**.
Description:	Enter a description for future reference if desired.

4. Click **OK**.
5. Assign devices to the case by clicking **Devices**.
6. Select the device to assign to the server(refer to "Add an IP Device" on page 13), click **Assign**, then **OK**.

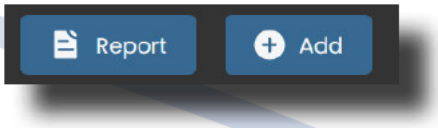
📖 When assigned to a case, IP devices may have their alias edited or used with an analytics engine.

7. Assign who has access to the case by clicking **Permissions**.
8. Select the desired users or user groups who will have access, click **Assign**, then **OK**.
9. Assign Auxiliary Devices to monitor on the case, by clicking Auxiliary Devices.
10. Select the desired devices to assign to the case, click **Assign**, then **OK**.
11. Click **Save** to exit.

📖 **NOTE**: As the case initializes, the status will be Recording-Pending, then Record-Active once ready. When transitioning to playback mode, the status will be Playback-Pending, then Playback-Active once ready.

Export Disk Usage Reports

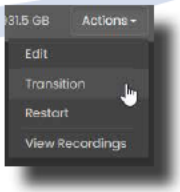
From the case list page, users may generate usage reports. For all available case disk usage information to export, click **Report** and the option to export to a .csv file will appear. To export reports for specific cases, type in a search entry, click **Report**, then **Download .CSV**.



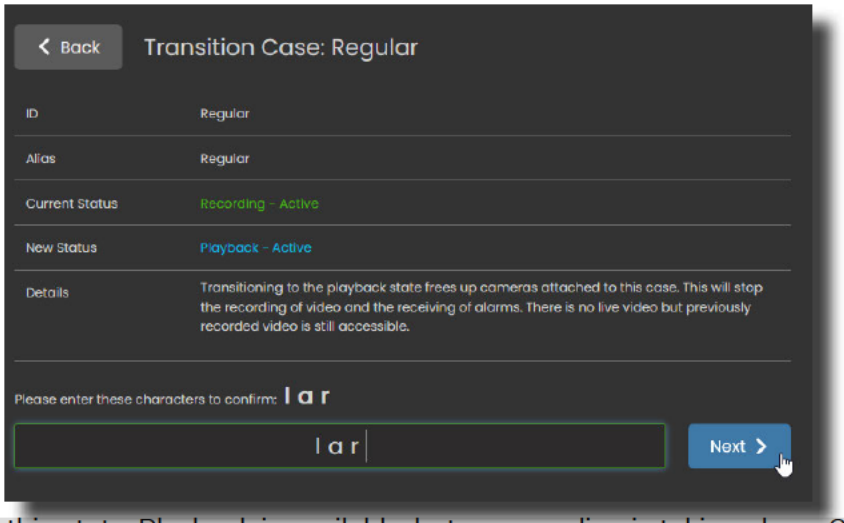
Transitioning a Case

Once case footage has been determined as completed, users may transition cases from active recording to playback mode. Playback cases may then be deactivated and archived before closing. **Airship's Video Archiver** must configured in order to archive footage. Refer to the ***Airship Archiver Quick Start Guide*** for setup instructions, or the ***Airship Archiver Quick Reference Guide*** for full archival process information.

1. To change the status of any case listed, click **Transition** in the **Actions** column.

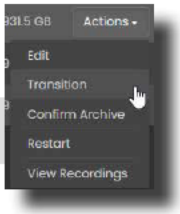


2. A prompt appears to confirm the status change to Playback-Active; enter the word above the open text field to confirm the transition, and click **Next**.



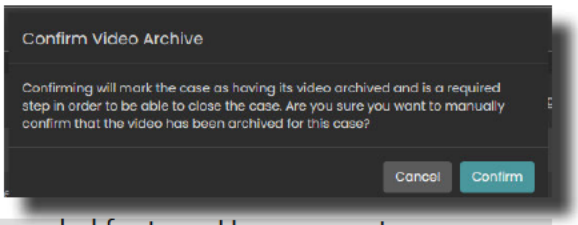
📖 **IMPORTANT:** In this state, Playback is available, but no recording is taking place. Cameras are free to be used elsewhere. This action cannot be undone; once a case has transitioned to playback mode, it cannot be set to record again.

3. A secondary confirmation is required, type "yes", then click **Transition**.
4. With the case status in **Playback-Active** mode, if it is desired to deactivate the case, click **Transition** once again.



📖 **IMPORTANT:** Select this option to stop and disable the case. Once deactivated, there is no way to go back to a previous state.

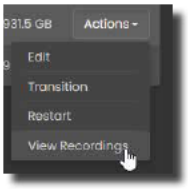
5. A confirmation message appears once again to confirm the transition to **Deactivated**.
6. With the case status in **Deactivated** mode, if it is desired to close the case, click **Confirm Archive**.
7. A warning message appears once again to confirm the transition to **Closed** (see image on right), click **Confirm**.



📖 **IMPORTANT:** Select this option to delete the case and all its recorded footage. Users cannot close the case until the recordings are archived. After the archival process is complete, choose this option to close the case. Closed cases cannot be re-opened.

Deleting Case Footage

From the case list page, click the **Actions** drop-down menu, and select **View Recordings**. The associated cameras assigned to the case will appear with each day of recording and may be selected individually or under the parent item. Select which items to delete, then click **Delete Recordings**.

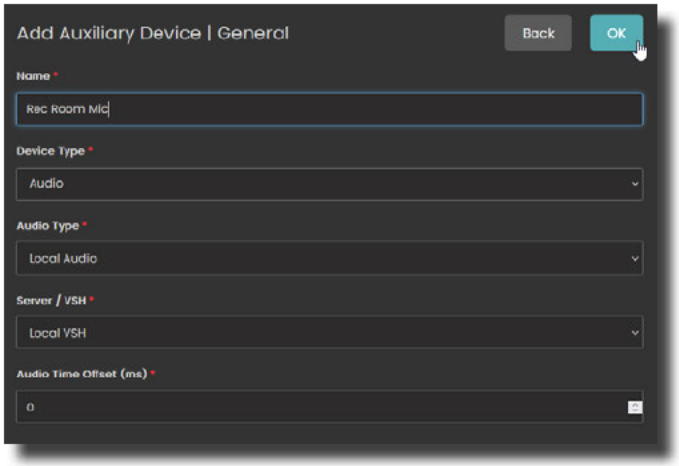


©2021 Airship Industries

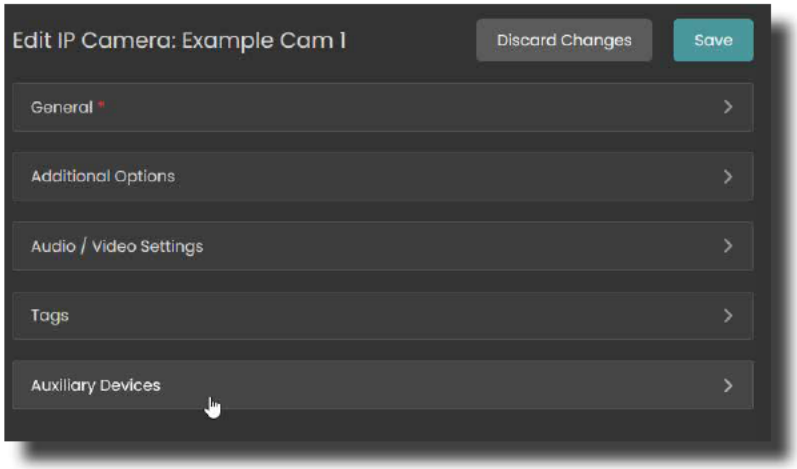
AUXILIARY DEVICES

Auxiliary devices such as microphones, PTT Radios, GPS-enabled device, or detectors may be added and assigned to IP cameras or cases, respectively.

1. From the main left-hand navigational menu, click **Auxiliary Devices**.
2. Click **Add**.
3. Enter a name and select the type of device to add. Select from Audio, GPS, Radio, or Detector (radars & sensors). Once the device is selected, options associated with that device appear.
4. Fill out all fields with a red asterick and click **OK,** then **Save**.



5. Assign the auxiliary device to an IP camera, case or VSH, respectively, by navigating to the desired instance, then click **Edit** from the **Actions** drop-down, then **Auxiliary Devices**.
6. Assign the device, then click **OK** and **Save**.



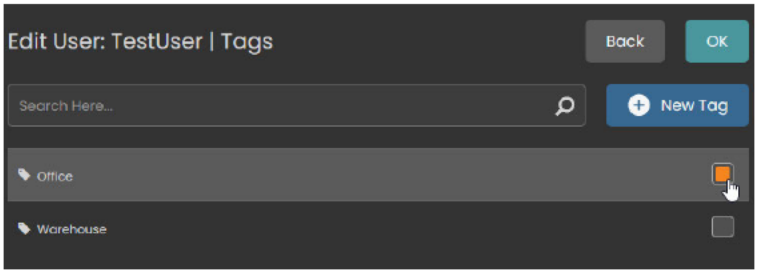
LOCATIONS AND TAGS

A system administrator can add locations and tags. Once locations and tags are created, they can be assigned to **VSHs**, **IP Cameras**, and **Users**. This enables searching assets by locations and/or tags.

Tags

Use tags to assist in sorting Users, IP Cameras or VSHs by the type of actions they take or the agency they are a part of. Examples might be "regional", "remote", the city and department, or countless other variations to help in sifting through large user lists.

1. Click **Tags** from the left-hand navigational menu.
2. Add a tag by clicking the **Add** button.
3. Name the tag, add a description if it is helpful for identification (not required), and click OK.
4. To assign the tag to a User, IP camera or VSH:
   - » Click **Users**, select the desired user, then click **Edit** from the **Actions** drop-down menu.
   - » Click **IP Cameras**, select the desired camera, then click **Edit** from the **Actions** drop-down menu.
   - » Open the **EMS Admin** menu, click **VSHs**, select the desired VSH, then click **Edit** from the **Actions** drop-down menu.
5. Click **Tags**.
6. Check the desired **Tags** for which to apply to the selected user, IP Camera or VSH, and click **OK**.



Locations

1. Click **Locations** from the left-hand navigational menu.

> 🕮 **IMPORTANT: Power Users** cannot create new locations. They can only see the location to which they belong.

2. Add a tag by clicking the **Add** button.
3. Name the location, add a description if it is helpful for identification (not required), and click OK.
4. To assign the location to a User, IP camera or VSH:
   - » Click **Users**, select the desired user, then click **Edit** from the **Actions** drop-down menu.
   - » Click **IP Cameras**, select the desired camera, then click **Edit** from the **Actions** drop-down menu.
   - » Open the **EMS Admin** menu, click **VSHs**, select the desired VSH, then click **Edit** from the **Actions** drop-down menu.
5. Click **General**.
6. Scroll down to select the desired **Locations** for which to apply to the selected user, IP Camera or VSH, and click **OK**.



©2021 Airship Industries

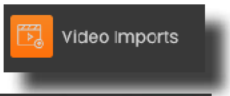
Locations Example

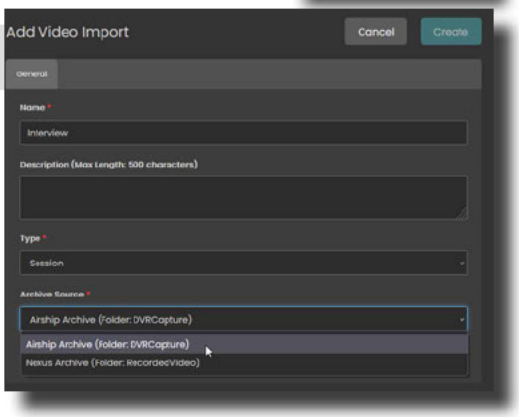
When many cameras, VSHs, and users are involved, locations can help to limit permissions to user-specific assigned locations. As an example, "Redmond" can be used as a location tag so that all users which are assigned to Redmond only have access to those defined cameras or virtual server hosts.

In order to set location-specific permissions, follow the directions above to assign a location to a VSH, then the desired cameras, then the user. When those three elements are in place, the assigned user can only access those cameras to which the location is assigned.

VIDEO IMPORTS

1. Click **Video Imports**, then click **+ Add**.
2. Enter a name for the video file.



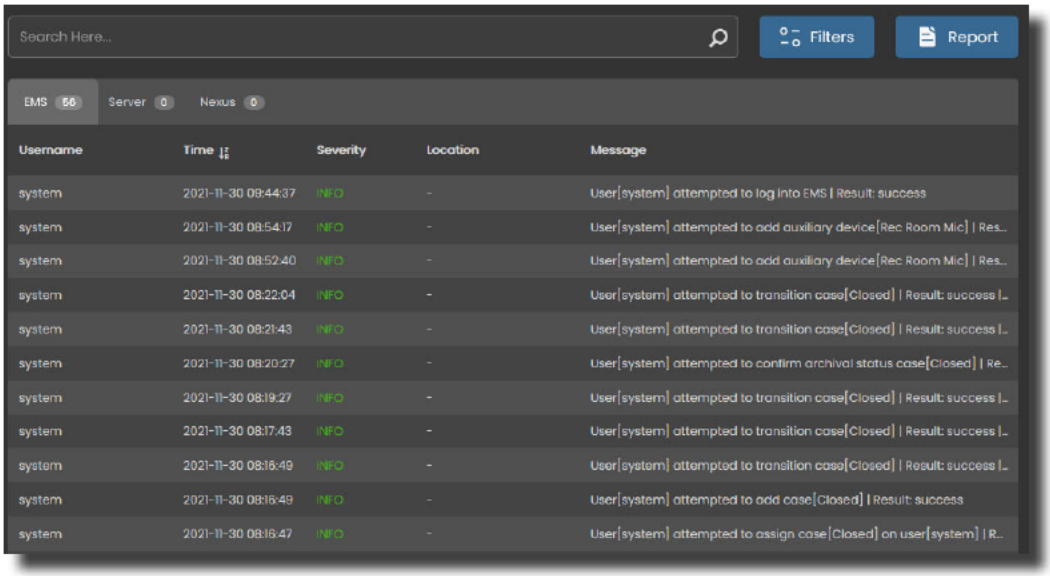


> 🕮 Session video import allows Airship VMS or Nexus VMS recording to be uploaded as a new playback case.

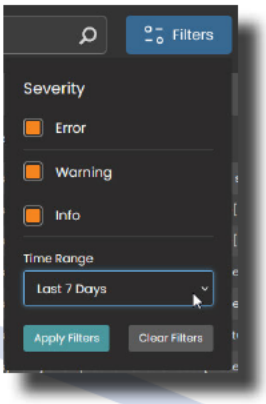
Interview video import allows MP4 clips to be viewable in Nexus Video Portal.

EVENTS

Logs are viewable in **EMS** in **Event Viewer** located on the left-hand navigational menu (click **Events**). Information regarding the user who triggered the event, the location it occurred in, as well as event time, severity, type, and message can all be found in the **EMS** Event Viewer. Also, the three tabs at the top allow the user to choose to view **EMS**, **Nexus Client**, or Server-related logs.



Click the **Filter +** Icon near the top-right corner to selectively filter the dates or type of alert for the selected application tab. Click **Error**, **Warning** or **Info**, select a time range, then click **Apply Filters**.



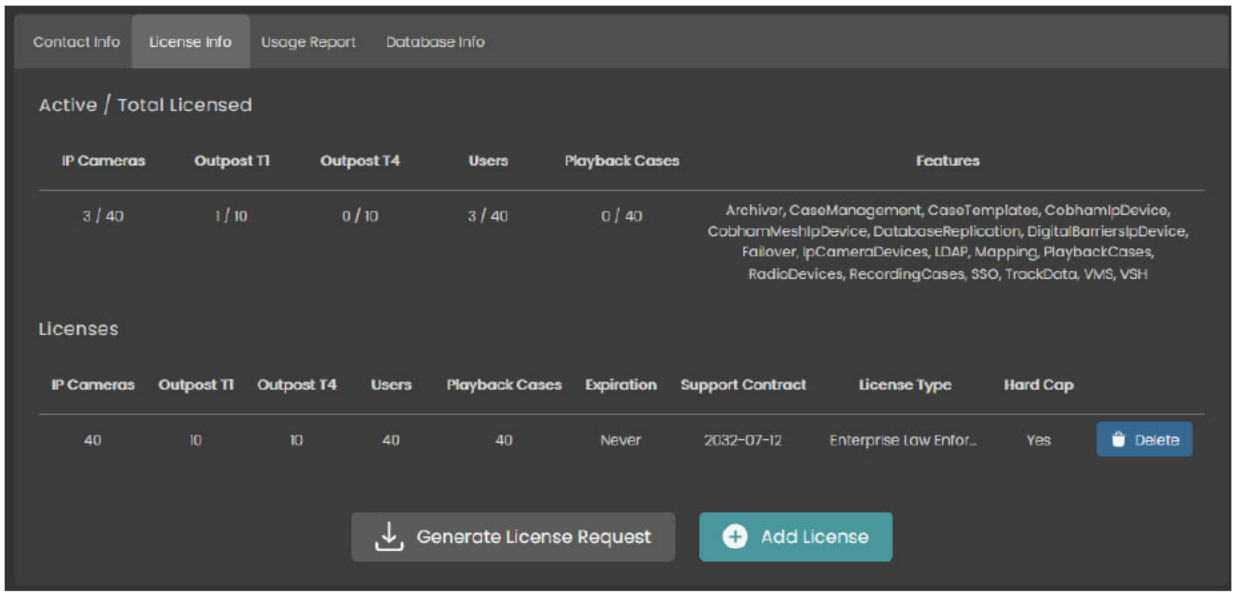
ABOUT

Contact Info

Contact Airship by phone or email using the provided contact information.

License Info

Information about the active license on EMS is displayed here. Under "Active/Total Licensed", each device has a maximum limit for licenses and displays the active devices in-use as a fraction. The number of active licenses, the start date, and type of contract is displayed under "Licenses".



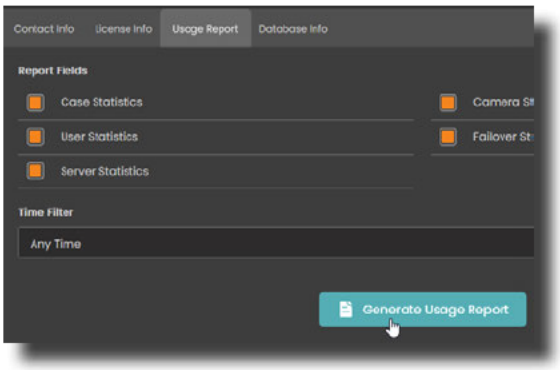
Genereate License Request: In order to add more servers, cameras, or Outpost devices to **EMS**, each user must have license. Click the **Generate License Request button** that will create a **LicenseRequest.dat** and Contact

📖 Contact **Airship** support to get your license validated.

Add License: After providing the **LicenseRequest.dat** file to **Airship** support, they will return a **managerlicensing.xml**. Save it to your desktop.

Usage Report

A CSV report may be exported for review purposes by clicking **Usage Report** > **Generate Usage Report** > **Export CSV**.

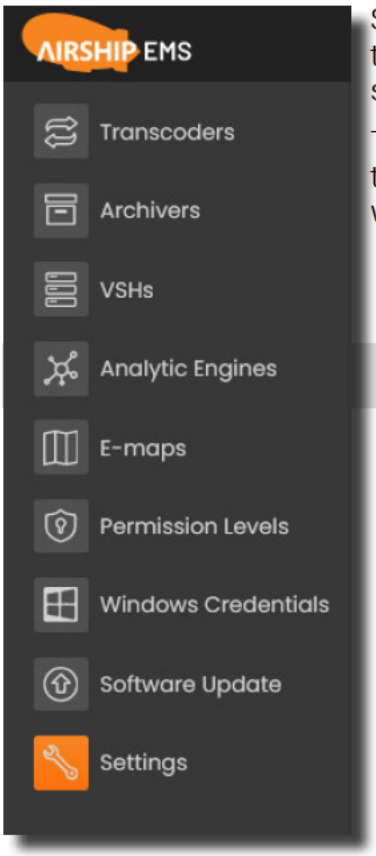


Database Information

Database Information is a tool that allows the user to see a list of all information about the current installation of the database.

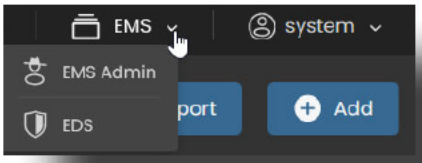
©2021 Airship Industries

SYSTEM ADMINISTRATOR ADVANCED OPTIONS



System Administrators have exclusive access to advanced configuration options. In the interest of streamlining routine System Administrator tasks, **EMS** separates this section from the rest of the options available to Power Users.

To open the System Administrator's menu, locate the EMS drop-down in the top right of the EMS window, anc click **EMS Admin**.



📖 **NOTE**: To exit the **EMS Admin** menu and return to the main menu, click the Airship logo, or click the **EMS Admin** drop-down, and select **EMS**.

Adding System Components

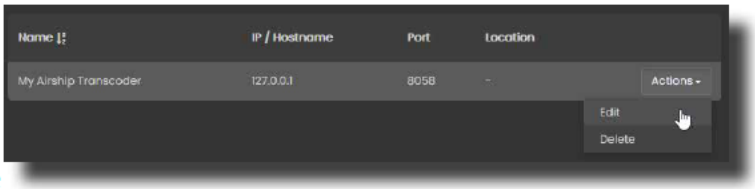
Airship's **Managed Setup Tool** automatically adds network-connected Airship components to **EMS** and manages them. Airship components such as Servers, Virtual Server Hosts, Transcoders, and/or Video Archivers are automatically detected and recognized. These components are added to either the **EMS** on network or to a standalone **Airship Server**.

To manually add **Airship** components such as additional **Servers**, **Virtual Server Hosts, Transcoders,** or **Video Archiver**, please refer to **Airship's *Managed Setup Tool Quick Start Guide***.

Transcoders

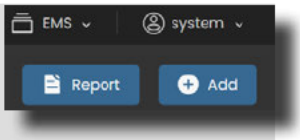
Transcoders convert audio/video formatting to a streamable feed which can be viewed on multiple platforms such as **Nexus Mobile**, **Video Portal**, and other **Airship** applications.

To edit the name, location, description, or permissions on a Transcoder, click the **Actions** drop-down and click **Edit**. Click the delete button to remove a Transcoder from **EMS**.

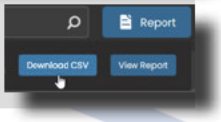


From the edit page, a System Administrator can edit the name, location, description, and **Permissions** assigned.

📖 A full list of Transcoders can be generated by clicking the **Report** button in the top right corner.



Select to download the report as a .csv file, or view the report from a web page.



Archivers

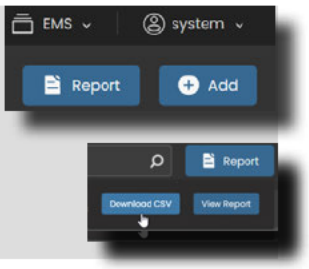
Archiver is installed automatically when **Airship Server** is installed on a specific computer, and is necessary for storing footage within cases. **Archiver** may be installed on any machine connected to the network and added with **EMS**.

1. To edit the name, location, description, or permissions on connected **Airship Archivers**, click **Archivers** from the **EMS Admin** menu.
2. From the list of available Archivers, and from the **Actions** drop-down, click **Edit** on the desired Archiver to edit.
3. From the edit page, a System Administrator can edit the name, location, description, and assign user **Permissions**.

📖 **IMPORTANT NOTE:** Make a note of the archiver computer's IP address as it will be entered into EMS settings.

📖 A full list of Archivers can be generated by clicking the **Report** button in the top right corner.

Select to download the report as a .csv file, or view the report from a web page.



Add Archiver to EMS:

Follow the prior section, "Adding System Components" on page 23 to add to **EMS** using **Managed Setup Tool**.

- When a new VSH is added, Video Archiver must be assigned in order to archive any videos from cases on that VSH. Administrators can add more than one VSH to a single Video Archiver if needed to archive videos from different cases.
- Archiving case video is mandatory before closing a case.
- Administrators can archive video (using **Airship's Archiver**) for any case currently in the Playback or Deactivated status.In **EMS**, users see the results of the archival operation.

Archiving Video

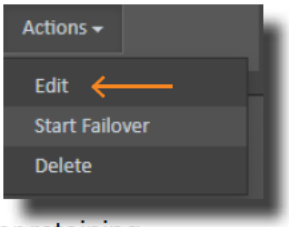
To export video to any external media device, connect the device before starting Archiver. Then follow the instructions in the ***Archiver Quick Reference Guide***.

©2021 Airship Industries

VSHs

A Virtual Server Host does just what its name implies: it "hosts" one or more Cases (as many as the hardware and network can handle). To add a VSH, follow the section, "Adding System Components" on page 23.

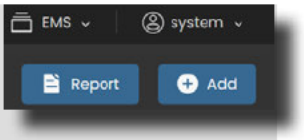
📖 **IMPORTANT**: VSHs can be managed to classic EMS, or to new EMS, not both.



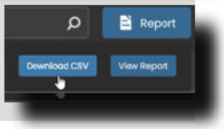
1. To edit existing **Virtual Server Hosts**, access the **EMS Admin** menu, and click **VSHs**.
2. Click the **Action** drop-down for the desired VSH, and select **Edit**.
3. Select from the available options to edit the following:

General:	Edit the VSH Name, Location, Timezone and Description.
Associations:	Choose a Transcoder (for viewing on web clients), Video Archiver (for retaining Archived footage), Standby VSH (for failover), or Analytic Engine to assign.
Permissions:	Select which User Groups may view the selected VSH.
Tags:	Assign a Tags or click **New Tag** to reference the VSH.

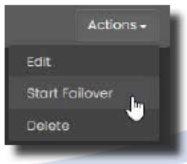
📖 A full list of VSHs can be generated by clicking the **Report** button in the top right corner.



Select to download the report as a .csv file, or view the report from a web page.



Failover Options



EMS provides the ability to failover an active/primary VSH which can be triggered either manually or automatically when the Airship Virtualization Agent stops communicating with **EMS** for a set number of minutes. When a failover occurs, the recording cases on the active/primary VSH will be initialized and started on a standby/failover VSH so that recording can continue. Upon recovering from a failover, the recording cases are stopped on the standby VSH and the active VSH will automatically handle the process of transferring the recording from the standby VSH to itself to keep everything together.



Failover setup and manual failover steps are covered in the ***Airship Failover Quick Reference Guide***.

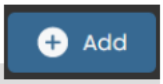
Analytic Engines

Airship integrates with leading edge detection software for facial recognition, license plate recognition, boat/hull and tail number recognition and continues to develop new partnerships. The analytic engines that process AI-based software can be added from the Analytic Engines section from the menu.
The process for adding analytic enginges for facial recognition or OCR capabilities are covered in the guides related to the associated integration feature, such as the ***Vintra Integration Quick Start Guide, or ALPR Setup Configuration Guide.***

E-Maps

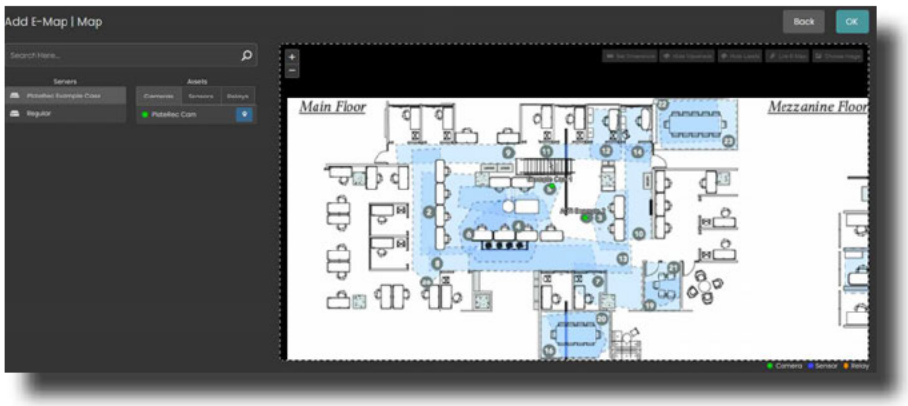
E-Maps are used to quickly picture camera orientation on a custom map. Users may upload an image by click E-maps, entering a name for the layout, and upload an image to later place cameras upon via **Nexus Client**. This feature is covered in detail in the **Nexus Client User Manual**, however a portion of this setup must be completed in **EMS**.

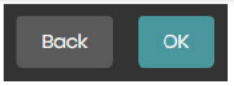
1. To upload a new map to place cameras upon in **Nexus Client**, click the blue **Add** button.

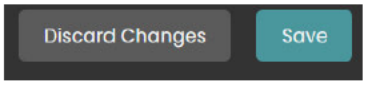


📖 If a map has already been added, click the **Actions** drop-down to edit.

2. Enter a name for the map, and click **OK**.
3. Click the outlined box on the right to upload an image to place cameras upon.
4. Select a Server or Case by clicking from the list on the left.
5. Click the box with a blue pin and then click again on the map to place orient the camera.
6. Click **OK**, then **Save**.





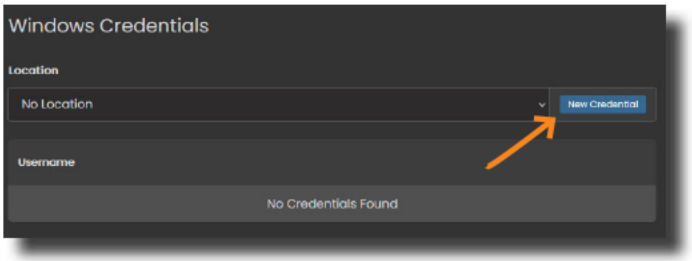


©2021 Airship Industries

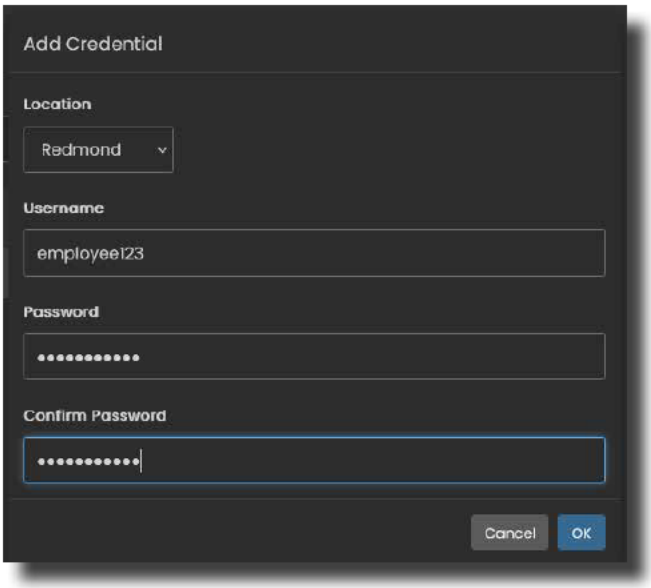
Windows Credentials

This page allows administrators to enter credentials that can be used for tasks such as encrypting tape archives through **Airship's Archiver** tool.

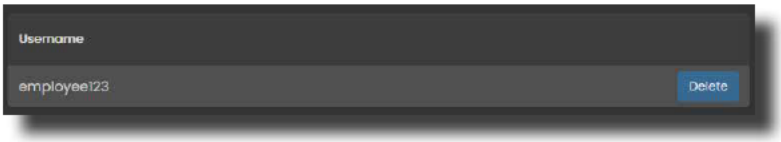
1. To add credentials, simply select a **Location**, and click **New Credential.**



2. Enter a username and password, and click **OK**.

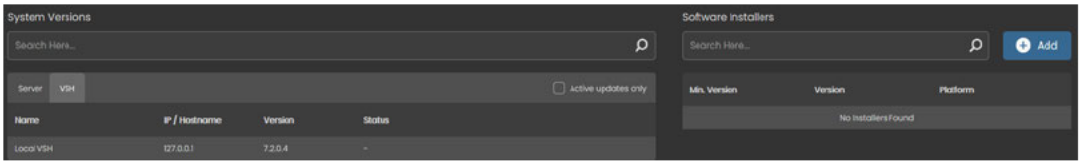


3. To remove a credential, simply choose the credential to be delete, and click the blue **Delete** button.



Software Update

The **Software Update** tab is used to upload new software versions from **EMS** to a given **VSH.** Upon uploading, EMS pushes the update to any VSH with an older software version.



System Versions

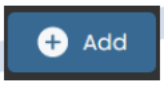
Click the **Software Update** option from the **EMS Admin** menu to display the list of softwares currently connected to **EMS**.

Name:	Displays the Server or VSH name.
IP/Hostname:	Displays the IP address or the hostname of the application.
Version:	Displays the version level of the application.
Status:	Displays the status messages about the application are available here.
Active Updates Only:	Check this box to show only those updates which are in progress.

Add Software Installers

Software Installers may be manually uploaded to EMS to ensure all versions of a given application are up to date. Listed below **Software Installers** is a list of all the software update packages currently in deployment for your management system.

To add a new Software Installer, click the **Add** button from the top-right.



Application:	Select the application that will be upgraded by this package. **Client** refers to **Nexus Client**, **DVR** refers to **Airship Server**, while **VSH** refers to the virtualized version of **Airship Server**.
Platform:	Select the Windows platform version on the installed machine (x86 for 32-bit systems, x64 for 64-bit systems).
Min. Version:	Enter the lowest version level of software acceptable to leave running on the system.
Version:	Enter the current version level of the package which will upgrade the application.
Select Package:	Upload the installer package by clicking the **Choose File** button.
Description:	Describe the installer for future reference, if so desired.

©2021 Airship Industries

Settings

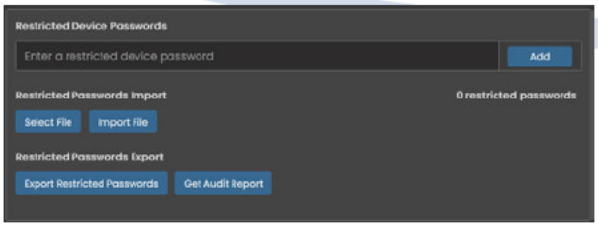
Click Settings from the left-hand navigational menu to view from the available options.

General

General settings for EMS requirements and options may be found by clicking "General" and are outlined below.

Manual Camera Numbering:	Check to allow manual entries for numbering cameras; otherwise camera numbers are automatically assigned. Nexus Client users may use camera numbers with keyboard shortcuts to call a camera.
Transcoder:	Select this option to disable transcoders from being added to EMS (not recommended).
Default EMS User:	Set to default Create User page to adding EMS Users, as opposed to LDAP (when enabled).
Require Locations:	Enable this to require a location to be entered for new users.
Require Case Archival:	Enable to require the automatic archival of all cases.
Inactive Session Timeout:	Set the desired length of inactivity – in minutes – before a user is logged out of **EMS**.
Enable Account Lockout:	Enabling this option locks out a user after a determined number of failed login attempts.
Custom Camera Fields:	This user-defined value can be anything which helps the user to identify specific information for the selected camera. Type an entry, then click **Add**. Click an entry, then **Remove** to delete entries.
Max Password Age:	Set the length in days until passwords expire. Setting this to 0 means this feature will not be used.
Enforced Password History Level:	The number of previous passwords that will be checked and disallowed when a user attempts to set a new one. Setting this to 0 means this feature will not be used.
Disable Inactive User:	Set the number of days until inactive users will be deactivated. Setting to 0 means this feature will not be used.
Days to Keep VMS Events:	Set the number of days to retain **VMS** triggered events in the database.
Days to Keep Nexus Events:	Set the number of days to retain **Nexus Client** triggered events on the server.
Days to Keep EMS Events:	Set the number of days to retain **EMS** triggered events on the server.
Automatic Failover Wait Time:	Set the number of minutes to wait for a VSH to come back online before automatically triggere a failover. Setting this to 0 means this feature is disabled.
Password Requirements:	Check this box for length, case, number, and character requirements; select the requirements below the box. ***Minimum Length*** (characters limit)***, Require Lowercase Character, Require Uppercase Character, Require Number, Require Special Number, Define Special Characters*** (defines characters to be considered "special")

Enable Device Password Restrictions: Passwords may be added to a list of restricted passwords to avoid commonly guessed or leaked passwords. Check the box, then either type in a password and click **Add** to disallow, or upload a complete list of passwords from a .csv file. To import a list of passwords, click **Select File**, then find the .csv to upload, and click **Import File**.



Further details may be found in the ***Airship Restricted Passwords Quick Reference Guide.***

Device Password Requirements: Check this box to enable password requirements for devices added to EMS, and select the desired requirements.

Two-Factor Authentication Type: Select the default authentication mode, using an Authenticator App such as Google Authenticator, by Email only, or Email and SMS, then see below.



Require Two-Factor Authentication: Set to require 2FA for users logging into **EMS**. Refer to "Two-Factor Authentication" on page 10. This requires the use of a QR scanning app and a 6-digit code entry.

Nexus Relay IP : The IP to be used for Outpost Mobile.

Nexus Relay Port: The port to be used for Outpost Mobile.

Use Local Nexus Relay IP: Check this box and enter the local IP if using Nexus Relay locally.

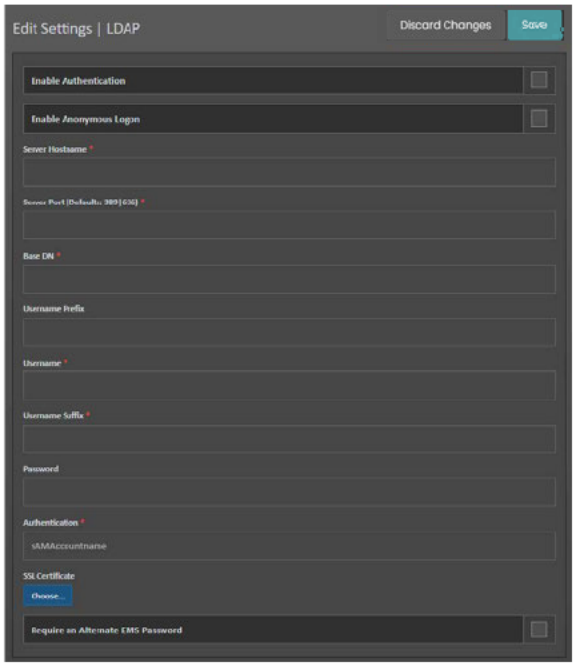
Default OCR Engine: Sets the default OCR Engine based upon what has been added from the Analytic Engines page.

Default Person/Vehicle Engine: Sets the default Person/Vehicle Engine based upon what has been added from the Analytic Engines page.

©2021 Airship Industries

LDAP Settings

Administrators can link users and user groups from active directory to **EMS**. Once you have a successful connection to the LDAP server, you can create users and user groups that are associated with LDAP login credentials.



To create a new user, refer to the Users section of this manual. On the **Add a User** page, enter the **Name** of the user as it appears in the LDAP directory and click the **link** button to validate the user exists in LDAP. If the user exists, all the user information along with username is fetched from the LDAP server to **EMS** and the user is created.

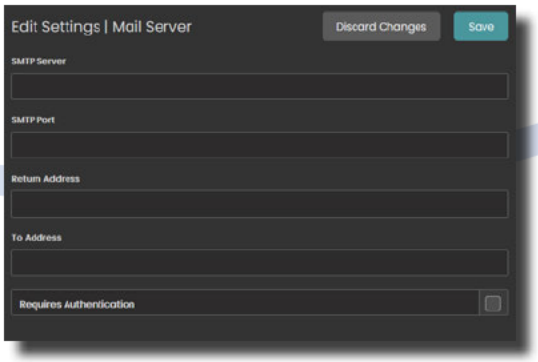
Once the user information is ready, the user can be added to any of the available user groups and assigned permissions. If an LDAP user logs in to **EMS**, a client, or the web client, that user's information, such as username and password, are sent to the LDAP server for validation (and marked as an LDAP user).

- A system administrator can link the LDAP users directly to new or existing **EMS** user groups. Then each user under the LDAP user group can log in to **EMS**. (They do not have to added again to the Users list in **EMS**).
- All the users of that LDAP group will inherit the permissions of the **EMS** user group.

Enabled Authentication:	Check this box to enable LDAP authentication that will enable or disable LDAP as part of **EMS**'s authentication.
Enabled Anonymous Logon:	Enable this field if your LDAP server is set to accept anonymous querying of its Active Directory (AD). You do not have to enter the LDAP username and password if you enable this option.
Server Hostname:	Enter the host name for LDAP server. It is typically ldap://xxx.xxx.xxx.xxx.
Server Port (default of 389, 636):	Enter the port number for your LDAP server. Default ports are 389, and 636 for SSL.
Base DN:	Enter the domain name where LDAP users are available. ***EXAMPLE:*** if your domain is 'airship.com', the base dn will be entered as 'dc=airship, dc=com'.
Username Prefix:	Deprecated. If you need a name for the admin user, it is recommended to enter it in the username field.
Username:	Enter the administrator username for LDAP login. If you enable **Enabled LDAP Anonymous Logon** option, this option is grayed out.
Username Suffix:	Deprecated. If you need a suffix for the admin user, it is recommended to enter it in the username field.
Password:	Enter the password for LDAP login.
Authentication:	This field displays your login name. Leave this option unchanged unless you know the specific one for your AD/LDAP configuration.
SSL Certification:	If you use SSL on your LDAP server, upload your certificate here. Browse through your computer and select the SSL certification.
Require Alternate EMS Password:	Check this box to Require a different password for logging into **EMS** than for other Applications.

Mail Server

Full email notification setup instructions can be found in the ***Email Notifications Quick Setup Guide***. Some settings within **Nexus Client** including which cameras will trigger events must be setup before any notifications will occur.



SMTP Server:	Enter the hostname/IP address of your SMTP Mail Server. Your network administrator can provide this information.
Port:	Default port for SMTP connection is 25.
Return E-mail Address:	Enter the address from which emails will be sent.
To Address:	Enter the email address where you would like alarm emails to be sent.
Requires Authentication:	Check this box if you want SMTP Server to authenticate the sent emails that require SMTP login, then enter the Username and Password.
Username:	Enter the username associated with login if authentication is required.
Password:	Enter the password associated with login if authentication is required.

©2021 Airship Industries

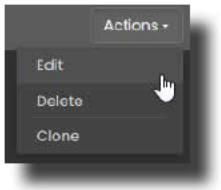
Permission Levels

Permissions to each application and each feature within applications may be individually assigned to existing user groups. To ***edit*** existing permission levels:

1. Click **Permission Levels** from the Advanced section of EMS.

📖 **NOTE**: Existing permission levels are assigned to each application. Hover the mouse over each permission to reveal tooltips explaining their uses.

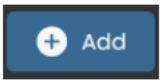
2. From the desired permission level, click the Actions dropdown, and select **Edit**.
3. Select the features for which to allow or prohibit access to by checking the box next to the feature.
4. Click **OK**.
5. Return to the main Dashboard, click Users, and edit the desired User to assign the permission set.



Custom Permissions

For custom permission levels, first create a group for which to assign unique permissions.

1. Click **Permission Levels**, then click the **blue Add** button.
2. Select which options to enable or disable by checking or unchecking the individual feature.



📖 **NOTE:** All "Manager" permissions refer to accessible features and options within the **EMS** user interface (UI). All "Client" permissions refer to connecting clients such as Nexus Client, Nexus Video Portal or Nexus Mobile. Finally, all "DVR" permissions refer to the standalone Airship Server or service (non-virtualized).

3. Click OK.
4. Return to the main Dashboard, click **Users Groups**, and edit the desired User Group to assign the permission set.

📖 See the ***Airship Permissions Quick Reference Guide*** for more information on assigning permissions. Hover the mouse over each permission to reveal tooltips explaining their uses.

GLOSSARY

Airship Server

Central to **Airship VMS**, **Airship Server** connects to cameras, sensors and other devices to collect and record video, audio and metadata for permission based distribution. This robust software is scalable for many use cases. It can be paired with other **Airship Servers** or run as a standalone system, additionally, it is capable of running multiple virtual instances simultaneously to securely manage extensive video, audio, and metadata input.

Archiver

An **Airship Server** based application that can archive video evidence in its raw format to a multitude of storage mediums such as disk, DVD, LTO/WORM tape, and other external media. Archived footage can be viewed directly using the included **Nexus Player** stored on each archive. Integration with Rimage Systems is also available. *Prerequisites: Airship Server*

Cases

Allows compartmentalization of groups of cameras to create a tailored workflow of preserving evidence. Cases preserve resources utilizing virtual instances of **Airship Server**; **Virtual Server Hosts**.

EMS

Airship's Enterprise Management System enables users to create and control tiered access levels, configure software (within the **Airship** ecosystem), cameras, devices, permissions, and other settings. **Airship EMS** scales to the size of the enterprise, whether large or small, camera/user groups and other helpful tools help organize day-to-day surveillance tasks across their networks. *Prerequisites: Server*

Nexus Client

This feature-rich viewing client enables user to view live and recorded footage, access alarm metadata, remotely configure cameras, pan/tilt/zoom, and numerous other features essential to surveillance monitoring. Installed on a desktop computer or laptop, this Windows software requires either a direct connection to the server's network or a valid VPN connection. The goal of **Nexus Client** is full control of camera feeds being recorded by **Airship Server**, while also offering remote server configuration capability. *Prerequisites: Airship Server*

Mobile Encoder

Mobile Encoder is a secure mobile app which provides end users the ability to stream live video and audio over cell or WiFi using their ios enabled mobile device. When used in conjunction with an **Airship Relay Server** and **Airship Server**, the stream can be recorded for playback via **Nexus Client** or **Nexus Mobile**.
Prerequisites: Airship Server, Relay Server, Nexus Client, iOS device

Outpost

Airship's edge-recording software; records high-resolution at the edge while sending a transcoded lower quality stream to an **Airship Server** via **Relay Server**. Allows for adaptive steaming settings based on your network connection allowing for the end user to get the best streaming quality possible from their network connection.

Nexus Video Portal

Nexus Video Portal allows for viewing live and playback audio\video recorded by **Airship Server** over a secure web connection. **Nexus Video Portal** can be accessed using any device which supports a modern browser.

Relay Server

Allows the user to securely connect to **Outpost** enabled edge devices without requiring a static IP address at the edge recorder, providing additional security for edge based data streams. *Prerequisites: Airship Server, Outpost*

Transcoder

Included with **Nexus Video Portal, Airship Transcoder** allows users to adjust their stream quality to better suite their connection speed. *Prerequisites: Airship EMS, Transcoder, Airship Server*

VSH - Virtual Server Hosts

Virtual Server Hosts are virtualized instances of **Airship Server**, which may be managed via **Airship's Enterprise Management System (EMS)**.

©2021 Airship Industries

NOTES



[end]
rev:202111301641

©2021 Airship Industries

Department of State Police
DIVISION COMMANDER'S ORDER

Issue Date	**Number**
May 3, 2022	**2022-DHS-002**
Subject: **Use of Non-Departmental ALPR Systems**	

The Division of Homeland Security and Preparedness is responsible for the administration of the Department's Automatic License Plate Recognition System (ALPR). The availability and use of ALPR technology provides opportunities to increase public and officer safety and to enhance the effectiveness of law enforcement agencies.

The Department shall only utilize ALPR technology in furtherance of official and legitimate law enforcement operations and public safety. The use of ALPR technology is governed by General Order TRF-11 "Automatic License Plate Recognition". In addition, the use of non-departmental ALPR systems shall be subject to the guidelines set forth in this Order until and unless superseded by General Order TRF-11.

In the course of their official duties, members may contact other law enforcement agencies to request assistance with information, records, or data from non-departmental ALPR systems.

Lieutenants and supervisory analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may access accounts with non-departmental ALPR systems for official law enforcement purposes as authorized by General Order TRF-11.

Other members, through their position with the Department, shall not obtain accounts with non-departmental ALPR systems unless authorized by the Division Commander of the Division of Homeland Security and Preparedness.

Members shall be mindful that non-departmental ALPR systems may use different technology and quality assurance standards than the Department's ALPR system.

_____

Christopher T. Wilcox
Lieutenant Colonel
Division of Homeland Security and Preparedness

NON-CRIMINAL JUSTICE AGENCY USER AGREEMENT
FOR ACCESS TO CRIMINAL HISTORY RECORD INFORMATION (CORI/CHRI)
between the
MASSACHUSETTS DEPARTMENT OF CRIMNAL JUSTICE INFORMATION SERVICES (DCJIS)
and

Agency Name		
Address		
City	State	ZIP Code
Full Name and Title of Agency Head		
Telephone Number		Fax Number
Email Address		

I. PURPOSE

This User Agreement identifies the duties and responsibilities of both the DCJIS and the non-criminal justice agency (hereinafter referred to as "NCJA" or "Agency") as they relate to the handling of requests and responses for state and national fingerprint-based criminal background checks.

The NCJA agrees to follow the terms of this agreement and will only submit requests for, review, and store CHRI background checks in accordance with 42 USC 16962, Public Law 92-544 and all other applicable federal and state laws and regulations.

II. THE PARTIES AGREE AS FOLLOWS

The DCJIS will:

1. Provide criminal history record information (CHRI) in response to submitted fingerprint-based background checks, either to the NCJA or to the appropriate agency that reviews criminal histories for the NCJA;

2. Provide assistance to the Agency in interpreting CHRI;

3. Work to ensure the completeness and accuracy of the CHRI;

4. Conduct audits to ensure compliance with this Agreement; and

5. Cease providing information to the Agency if this Agreement is violated or if the Agency is suspected of violating this Agreement.

The NCJA will:

1. Abide by the terms and conditions identified in this Agreement;

2. Abide by the terms of the current version of the FBI CJIS Security Policy (CSP) and any subsequent versions;

3. Comply with state and federal laws, rules, procedures, and policies, including those adopted by the DCJIS and the National Crime Prevention and Privacy Compact Council (Compact Council) regarding the use and dissemination of CHRI;

4. Use CHRI only for the purpose requested;

5. Submit requests for CHRI checks only as authorized by law;

6. Provide for the security of any criminal history record information received. This includes, but is not limited to:

    a. designating a Local Agency Security Officer (LASO) who is responsible for ensuring compliance with security procedures and this User Agreement.
    b. ensuring all personnel with access to CHRI are aware of the rules and responsibilities with regard to CHRI and have completed the required training.
    c. restricting access to physical or electronic copies of CHRI to authorized personnel. Physical copies shall be maintained in a controlled, secure environment, such as a locked cabinet in a room not accessible to all staff and visitors. Electronic copies shall be protected with at least 128-bit encryption. The relevant federal encryption standard is FIPS 140-2.
    d. sharing CHRI only when explicitly allowed by law and logging any CHRI dissemination. Logs shall include, at a minimum, the subject's name, the subject's date of birth, the date and time of dissemination, the name of the person to whom the CHRI was disseminated along with the name of the organization for which the person works, and the specific reason for dissemination.
    e. tracking and reporting information security incidents, such as the theft/loss of physical records or the penetration of electronic systems.
    f. disposing of CHRI in the required, secure manner. Physical media must be cross-shredded and/or burned, and electronic records must be deleted and repeatedly over-written with random 0s and 1s, or the media must be degaussed.

7. Understand this data is based on CHRI received by the DCJIS. If a person could be adversely affected by this data, the person must be given the opportunity to challenge and correct a record before a final decision is rendered on the basis of the CHRI;

8. Retain audit records for at least 365 days. Once the minimum retention time period has passed, the agency shall continue to retain audit records until they are no longer needed for administrative, legal, audit, or other operational purposes;

9. Allow the DCJIS and the FBI to conduct audits to ensure compliance with this Agreement; and

10. Respond to, and cooperate with, the investigation of any complaints alleging a violation of this agreement or of the laws, regulations, and policies regarding access to, and use of, CHRI information.

III. CRIMINAL HISTORY RECORD INFORMATION LIMITATIONS

The NCJA understands that CHRI has the following limitations:

1. CHRI is based solely upon arrest fingerprint cards submitted to the Massachusetts State Police (MSP) State Identification Section (SIS) and to the FBI. The arrest warrant file, sex offender file, or other databases maintained by the DCJIS are not part of the CHRI search.

2. CHRI is compiled from information submitted to the MSP SIS and to the FBI by law enforcement agencies (hereinafter referred to as contributing agencies). Although the MSP SIS makes reasonable efforts to ensure all information is submitted as required by State law, it is not responsible for omissions from contributing agencies.

3. Although the MSP SIS encourages the reporting of all arrests for felony, misdemeanor, and drug violations, Massachusetts law enforcement agencies are only required to submit fingerprints on felony and drug-related arrests.

4. CHRI is constantly being updated as new arrests and other information are entered into the system by contributing agencies. The record released is only valid as of the date the record check was performed.

5. Certain statutes allow for the suppression or deletion of records, and this information is not provided.

6. The MSP SIS retains records for the State of Massachusetts only. Most fingerprint-based background checks include a check through the FBI, which the MSP SIS will request on the NCJA's behalf as a normal part of the criminal background check, if allowed by law.

IV. PERSONNEL SECURITY AND TRAINING REQUIREMENTS

Individuals within the NCJA who have direct access to CHRI or to systems containing CHRI are subject to criminal history record checks performed by the DCJIS. The NCJA agrees to ensure that all affected personnel are screened as provided in this agreement.

Access will be denied if the individual has ever had a felony conviction of any kind, no matter when it occurred. Access may be denied if the individual has one or more recent misdemeanor convictions. In addition, an individual believed to be a fugitive from justice, or having an arrest history without convictions, will be reviewed to determine if access to CHRI is appropriate. The DCJIS will take into consideration extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

In addition to the above, CHRI access will be discontinued for any person who is subsequently arrested for, or convicted of, a crime. The NCJA's Local Agency Security Officer (LASO) must report such incidents to the CJIS Systems Officer at the DCJIS for review before access may be reinstated. The NCJA further agrees that where authorized by law, support personnel, contractors, vendors, and custodial workers with access to controlled areas during CHRI processing will undergo state and/or national criminal background checks unless escorted by authorized personnel at all times.

The LASO will be responsible for reporting all personnel security clearance requests and issues to the DCJIS CSO within five (5) business days.

An informed review of CHRI results requires training. As such, the NCJA agrees that all authorized personnel, including those personnel with direct access to SAFIS-R and those that will access SAFIS results, will complete the required training and review all training materials made available by the DCJIS every two years. Furthermore, all authorized personnel must also execute a Criminal Record Information (CORI/CHRI) Individual Agreement of Non-Disclosure (AOND) form.

V. PHYSICAL AND ELECTRONIC SECURITY OF CHRI

The NCJA is responsible for ensuring the physical and electronic security of CHRI at all times. Therefore, the NCJA must adhere to the following:

1. CHRI shall only be processed in controlled areas with limited access.
2. Computers which provide access to CHRI data shall not be logged in when unattended.
3. Authorized users shall not share Usernames and Passwords.
4. Documents shall not be left out in the open as they could be viewed by unauthorized individuals.
5. Computer screens and CHRI shall not be viewable by unauthorized individuals.
6. File cabinets and record rooms shall be locked when unattended.

VI. INCIDENT RESPONSE REQUIREMENTS

A "security incident" is defined as (a) unlawful or unauthorized access to, and/or dissemination of, any CHRI stored on the NCJA's equipment or in the NCJA's facilities resulting in access to, or loss, disclosure, or alteration of, CHRI, or (b) unlawful or unauthorized access to such facilities or equipment resulting in access to, or loss, disclosure, or alteration of, CHRI.

The NCJA LASO shall report any and all security incidents to the DCJIS Information Security Officer (ISO) within 48 hours of the discovery of the incident.

VII. DOCUMENT SIGNOFF

This Agreement commences on the date the last signature is obtained below and continues until terminated by one of the parties. Written notice of one of the parties' intent to terminate this agreement must be submitted at least 14 days prior to the termination date. This Agreement may be terminated sooner by the DCJIS upon a violation of the terms of the Agreement.

NON-CRIMINAL JUSTICE AGENCY

Signature of Agency Head	Date
Title	
Print or Type Name	

MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

Signature of CJIS Systems Officer, DCJIS	Date
Print or Type Name Jamison R. Gagnon	

Submit the completed Agreement via U.S. Mail or via email to:

Massachusetts Department of Criminal Justice Information Services
ATTN: SAFIS Unit
200 Arlington Street, Suite 2200
Chelsea, MA 02150
Telephone: 617.660.4790
Email: safis@mass.gov

THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

OFFICE OF THE ATTORNEY GENERAL
ATTORNEY GENERAL MAURA HEALEY



A PROJECT OF THE CRIMINAL BUREAU
DIGITAL EVIDENCE LABORATORY
APPEALS DIVISION

JUNE 2021

A NOTE TO READERS OF THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

The Massachusetts Digital Evidence Guide (hereinafter "Guide") is only to be used as an educational resource. This Guide is not legal advice. The purpose of this Guide is to provide the reader with an understanding of the Massachusetts statutes and cases impacting criminal investigations and prosecutions that involve technology or digital evidence. This Guide, and its provisions, are not policy. This Guide does not suggest modifying or replacing any existing agency practices or procedure(s). Readers should consult with appropriate authorities, prosecutors, or legal counsel for necessary legal advice, case or statutory interpretation, or implementation of the document for any internal use. Readers who intend to rely on cases and statutes cited in this Guide should consult with the source document, confirm the interpretation, and investigate subsequent history. Questions or comments about, or suggestions for this Guide can be e-mailed to agodel@mass.gov.

THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

Office of the Attorney General, Maura Healey

Contents

Contents 2

I. Investigation 7

A. The Search and Seizure of Digital Evidence 7

1. Was There a Search or Seizure? 7

a) Searches and the Reasonable Expectation of Privacy 8

(1) Standing 8

(2) One Party Consent 9

(3) The Third-Party Doctrine 9

(4) Surveillance in Public: Public View Principle, Mosaic Theory, and More 13

(5) Peer-to-Peer and Other Network File Sharing 14

(6) Expectation of Privacy in Data That Is Not One's Own 16

(7) Probationers, Parolees, and Court-Ordered Monitoring 17

b) Seizures and Interference with Possessory Interest 19

c) Private Party Searches 20

(1) Initial Search Made by Private Party 20

(2) Warrantless Search: Private Citizen or State Actor 21

(3) An ISP's Reporting Obligation Does Not Make it a State Agent 22

2. Was a Search or Seizure Reasonable? 22

a) Warrants 22

(1) Probable Cause / Affidavit 23

(2) Independent Source Doctrine 30
(3) Particularity / Scope 31
(4) Staleness of Information Supporting Probable Cause 36
(5) Timely Execution of the Warrant 38
(6) Manner of Executing the Warrant 39
b) Exceptions to the Warrant Requirement 40
(1) Search Incident to Arrest 40
(2) The Plain View Doctrine 42
(3) Exigent Circumstances 44
(4) Emergency Aid Exception 45
(5) Inventory Exception 46
(6) Consent 47
3. The Exclusionary Rule 48
a) Good Faith / Substantial and Prejudicial 48
b) Inevitable Discovery 49
B. Search of Electronic Service Providers 49
1. General Overview of Stored Communications Act 49
2. Search warrants served on out-of-state Internet service providers 50
C. Encryption and Self Incrimination 50
1. The Foregone Conclusion Doctrine 50
2. Encryption 51
3. Sample Decryption Protocol 54
D. Searches Implicating Attorney-Client Privilege 54
1. Post-Indictment Email and File Searches 55

2. Taint Teams 55
3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails) 56
II. Evidentiary Matters 57
A. Judicial Discretion 57
1. Trial Judge's Discretion 57
2. Demonstrative Photographs 57
B. Discovery 57
1. Pornographic Images in Child Pornography Cases 57
2. Wiretap transcripts 58
3. Cell phone data 58
C. Authentication 59
1. Generally 59
2. Photographs and Digital Images, Videos, and CDs 59
3. Digitally Enhanced Images and Video 60
4. Transcripts of Recordings 60
5. Email 61
6. Chatrooms 62
7. Text Messages 62
8. Information Available on Websites and Social Networks 62
9. Software Programs Used in Investigation 64
10. GPS and Probation 64
D. Technological evidence as the basis of criminal conviction 65
E. Best Evidence Rule 66
1. Best Evidence Rule - Generally 66
2. Digital Images 66

3. Admission of Duplicate Evidence 66
4. Videos 67
5. Email 67
6. Summaries 67
F. Hearsay 68
G. Business Records Exception 68
1. Email 68
2. Computer Records 69
H. Confrontation Clause 69
1. Software-generated information 69
2. Secondary Examiners 70
III. Cybercrimes 72
A. Possession of Child Pornography 72
1. Multiple Convictions Require Multiple "Caches" 72
2. Brief Possession is Sufficient 72
3. Receipt by Cell Phone is Sufficient 73
4. Malware and Computer Viruses Defense 73
5. Probable cause / Staleness in Child Pornography Cases 73
B. Statutory Terms of Mass Gen. Laws ch. 272 74
1. "Dissemination" 74
2. Computer "Depictions" 74
3. Child Enticement 75
4. "Visual Material" 75
5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31 75
6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A 75

7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A 76
8. Lewdness 77
C. Special Conditions of Probation 77
IV. Expert Testimony About Technology 79
V. List of Cases Organized by Device/Evidence Type 80
A. Cell Phone Searches 80
B. Search of Computer Files 80
C. Email 80
D. CSLI, GPS, and Other Location Technologies 81
E. Text Messages 81

I. Investigation

A. The Search and Seizure of Digital Evidence

As with physical evidence, searches and seizures of digital evidence must be reasonable to be valid. This section provides a summary of Fourth Amendment law as it relates to the search and seizure of digital evidence. It also references Article Fourteen of the Massachusetts Declaration of Rights, which parallels the Fourth Amendment, but is sometimes more expansive.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Article Fourteen (art. 14) of the Massachusetts Declaration of Rights is similar to the Fourth Amendment, but since 1985, the Supreme Judicial Court ("SJC") has interpreted it as providing broader protections than its federal counterpart. Commonwealth v. Upton, 394 Mass. 363, 373 (1985) ("We conclude that art. 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause.").

To determine whether law enforcement action constitutes an unreasonable search or seizure, courts ask two questions. First, was the action a search or seizure within the meaning of the Fourth Amendment? E.g., Commonwealth v. Magri, 462 Mass. 360, 366 (2012) ("In deciding whether police conduct violates the Fourth Amendment or art. 14 of the Massachusetts Declaration of Rights, we first determine whether a search, in the constitutional sense, has taken place."). Second, was that search or seizure reasonable? See, e.g., Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness." (internal quotation marks omitted)).

1. Was There a Search or Seizure?

"A search implicating the Fourth Amendment occurs 'when an expectation of privacy that society is prepared to consider reasonable is infringed' and a seizure of property for purposes of the Fourth Amendment occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'" Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (quoting United States v. Karo, 468 U.S. 705, 712 (1984)) (finding installation and use of a GPS tracking device on a car to be a seizure under Massachusetts art. 14 because it requires entering the vehicle and using the electricity of the defendant's car).

a) Searches and the Reasonable Expectation of Privacy

For a search to implicate the Fourth Amendment, the defendant must have a "reasonable expectation of privacy" in the place to be searched. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); see also United States v. Heckencamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding a college student had a reasonable expectation of privacy in the contents of his personal computer because it was located in his dorm room, was protected by a password, and was not subject to regular university monitoring). A person's expectation of privacy is reasonable "if he can demonstrate a subjective expectation that his activities would be private, and he can show that his expectation was one that society is prepared to recognize as reasonable." Heckencamp, 482 F.3d at 1146 (internal quotation marks, brackets, and citations omitted). Individuals generally have a reasonable expectation of privacy in their personal computers and files. See id. at 1146–47 (listing cases to that effect). In Heckencamp, "[t]he salient question [was] whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network." Id. at 1146.

When challenging the constitutionality of a search, the defendant bears the initial burden of establishing that a search occurred. See Commonwealth v. D'Onofrio, 396 Mass. 711, 714-15 (1986); Commonwealth v. Alvarez, 480 Mass. 1017, 1018 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer).

The sections below explore the contours of the reasonable expectation of privacy, discussing: (1) standing; (2) one-party consent; (3) the third-party doctrine; (4) surveillance in public; (5) file sharing over networks; (6) reasonable expectations of privacy in data that is not one's own; and (7) diminished privacy expectations in the context of probationers, parolees, and court-ordered monitoring.

(1) Standing

Standing to challenge a warrantless search or seizure may be in question when the location or item searched or seized does not belong to the challenging party.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully suppressed CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105, 107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Commonwealth v. Almonor, 482 Mass. 35 (2019), the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Almonor, 482 Mass. at 47-48 (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The Court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have

automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because, "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Id. at 108. The Court found that the defendant did have standing to challenge the search of his own cell phone, but the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 108-09.

(2) One Party Consent

In Massachusetts, "one party consent" does not negate a reasonable expectation of privacy of the non-consenting party. While the Supreme Court held that warrantless electronic surveillance with "one party consent" does not implicate the Fourth Amendment, United States v. White, 401 U.S. 745, 751 (1971), the SJC found such surveillance impermissible under art. 14 of the Massachusetts Declaration of Rights, Commonwealth v. Blood, 400 Mass. 61, 70 (1987). Because it found there is a reasonable expectation of privacy in conversations that occur among "a narrow compass of known listeners" in private homes, the SJC concluded that the warrantless electronic surveillance was a violation of that constitutional provision. Id. Accordingly, "one party consent" did not obviate the need for a warrant under art. 14. Id.

(3) The Third-Party Doctrine

In United States v. Miller, 425 U.S. 435 (1976), and Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court articulated what has become known as the "third-party doctrine." Under this doctrine, "the Fourth Amendment does not prohibit the obtaining of information revealed [by a suspect] to a third party and conveyed by him to Government authorities," regardless of the suspect's expectation of how the information might be used. Miller, 425 U.S. at 443. Massachusetts has traditionally followed the Supreme Court's guidance on the third-party doctrine. See, e.g., Commonwealth v. Cote, 407 Mass. 827, 833–36 (1990) (holding that a defendant had no reasonable expectation of privacy in telephone message records held by a third-party answering service for the reasons cited in Miller).

- United States v. Jones, 565 U.S. 400 (2012). Unanimous decision holding that a Fourth Amendment "search" occurs where law enforcement places a GPS device on defendant's car. Id. at 411. The Court's opinion, authored by Justice Scalia, focused on the Government's intrusion on the defendant's physical property and applied "an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted." Id. In contrast, Justice Sotomayor's concurrence in Jones emphasized that "the Fourth Amendment is not concerned only with trespassory intrusions on property," id. at 954, and brought the issues later addressed by Carpenter v. United States, 138 S. Ct. 2206 (2018), to the forefront, see Jones, 565 U.S at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age…").

Carpenter v. United States, 138 S. Ct. 2206 (2018) and Commonwealth v. Augustine, 467 Mass. 230 (2014) modified the third-party doctrine for at least one specific type of information—cell site location information ("CSLI"). The holding of Carpenter is that law enforcement effects a Fourth Amendment "search" by obtaining at least one week's worth of a defendant's CSLI from a third-party cellular provider. See Carpenter, 138 S. Ct. 2206, 2217 n.3. The comparable holding from Augustine is that subpoenaing two weeks' of CSLI information is a "search." See Augustine, 467 Mass. 230, 233, 255 (2014).

- Carpenter v. United States, 138 S. Ct. 2206 (2018). The Government successfully applied for two court orders directing Carpenter's wireless carriers to disclose Carpenter's CSLI for select time periods within a four-month span. 138 S. Ct. at 2212. The first order sought 152 days of CSLI from MetroPCS, and the second order sought seven days of CSLI from Sprint. Id. Based in part off the information the Government acquired from Carpenter's CSLI, the Government charged Carpenter with six counts of robbery and six counts of carrying a firearm during a federal crime of violence. Id.

  The Supreme Court held that the Government's acquisition of Carpenter's CSLI was a search of Carpenter that required a warrant supported by probable cause even though the Government acquired the CSLI from third-party wireless carriers. Id. at 2221. The Court declined to apply an expansive version of the third-party doctrine to CSLI partly because the data can reveal immense amounts of intimate information about who a suspect has been associating with and where a suspect has been travelling. Id. at 2219 ("There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today."). Furthermore, because cell phones are a nearly ubiquitous part of daily life and virtually every activity on a phone generates CSLI, the Court rejected the claim that Carpenter voluntarily disclosed his CSLI to his wireless carriers. Id. at 2220 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term.").

  While the Court stated that its ruling was "a narrow one" that applied only to CSLI, id., the dissents argued that the decision will have far-reaching consequences, e.g., Carpenter, at 2234 (Kennedy, J., dissenting) ("The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties."); see also id. at 2262 (Gorsuch, J., dissenting) ("Today the Court suggests that Smith and Miller distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to 'extend' those decisions to particular classes of information, depending on their sensitivity." (emphasis in original)); cf. Commonwealth v. Augustine, 467 Mass. 230, 253 (2014) (holding that although "we do not reject categorically the third-party doctrine," some forms of electronic evidence require "a different approach"). Given Americans' increasing dependence on technological devices that generate large amounts of personal data, it is possible that the Supreme Court's reasoning in Carpenter will someday result in a larger overhaul of the third-party doctrine.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case similar to Hobbs, considering retroactive application of Augustine's warrant requirement for CSLI data, the SJC again held constitutional a pre-Augustine CSLI request because the associated 18 U.S.C. § 2703 application satisfied the requisite probable cause standard. Id. at 166-72.

- Commonwealth v. Almonor, 482 Mass. 35 (2019). This case concerned an issue of first impression involving whether police action that causes an individual's cell phone to transmit its real-time location information violates any reasonable expectation of privacy. Id. at 41. Neither the Supreme Court's decision in Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018) nor the SJC's decision in Commonwealth v. Augustine, 467 Mass. 230, 4 N.E.3d 846 (2014) addressed this precise issue. The Commonwealth charged the defendant with murder after he shot and killed an individual and subsequently fled the scene of the crime. After a witness gave them the defendant's phone number, the police filed a "mandatory information for exigent circumstance requests" form with the telephone service provider. The telephone service provider "pinged" the defendant's phone and revealed the defendant's GPS coordinates to the police. Id. at 38-39. The Court granted the defendant's motion to suppress the warrantless "pinging." Id. The SJC reversed, holding that the warrantless pinging of the defendant's phone constituted a search under the Article 14 of the Massachusetts constitution, but that the warrantless search was justified by exigent circumstances, namely that the defendant was at large and believed to be armed and dangerous. It noted that searches occur when the government intrudes on a person's reasonable expectation of privacy and concluded that the defendant had a reasonable expectation of privacy in his cellular location data. Id. at 43-44. The Court held that real-time location data serves as a "proxy for the real-time location of the individual" because "cell phones are an indispensable part of daily life and exist as almost permanent attachments to their users' bodies." Id. at 45 (internal quotations omitted).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). In 2011, the government received historical CSLI from defendant's cell service provider pursuant to a 18 U.S.C. § 2703 order, without a warrant — well before 2014, when Augustine first articulated the warrant requirement for historical CSLI requests. Id. at 542-44. The SJC held that the government could "still satisfy the warrant requirement if it can establish that its 'application for the § 2703[] order met the requisite probable cause standard of art. 14,'" i.e., the same probable cause standard required of an affidavit in support of a search warrant for historical CSLI. Id. at 544 (quoting Augustine, 467 Mass. at 256). (This also comports with Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016), an earlier case considering retroactive application of Augustine to CSLI data obtained pre-Augustine pursuant to an 18 U.S.C. § 2703 order.)

- Commonwealth v. Fulgiam, 477 Mass. 20 (2017). In Fulgiam, the Commonwealth obtained recent text messages of the defendant pursuant to § 2703(a) of the Federal Stored Communications Act. Id. at 28; 18 U.S.C. § 2703(a) (2012). The Court held, on federal statutory and state constitutional grounds, that law enforcement required a warrant to obtain the text messages. See 477 Mass. at 31. An individual under Massachusetts state law has a "reasonable expectation of privacy in his text messages." Id. at 33. The third-party doctrine did not require

otherwise because "the nature of cellular telephone technology . . . [and] use in our current society render the third-party doctrine inapposite" in this context. Id. at 34.

- Commonwealth v. Estabrook, 472 Mass. 852 (2015). The SJC considered a request for CSLI and concluded that a defendant's reasonable expectation of privacy under art. 14 of the Massachusetts Declaration of Rights is not violated by a warrantless request for production of up to six (6) hours of historical CSLI. Id. at 854. It also established that the relevant consideration in determining the reasonable expectation of privacy is the length of time for which CSLI data is requested, not the time span ultimately sought to be introduced at trial. Id. at 858–59.

- Commonwealth v. Augustine, 467 Mass. 230 (2014). Police investigating a murder obtained the defendant's CSLI from his service provider pursuant to a 18 U.S.C. § 2703(d) order. Id. at 233. These orders are not warrants, so they cannot be used to effectuate a search for information protected by the Fourth Amendment or art. 14. The CSLI obtained helped police determine the defendant's location over the period they were investigating. See id. at 233–34. The Court considered but ultimately rejected the Commonwealth's argument that the third-party doctrine negated any reasonable expectation of privacy the defendant had in his CSLI. Id. at 241–56. It reasoned that art. 14 does not protect information voluntarily and intentionally transmitted to third parties (like the number dialed to initiate a call) but it does protect information incidentally transmitted (like the location information the cell phone provider acquires as a result of cell phone technology). Id. at 249–52. The Court found that the defendant therefore had a reasonable expectation of privacy in his CSLI, which, under art. 14, means that "the government must obtain a search warrant to obtain it." Id. at 252.

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). Law enforcement obtained thousands of emails related to fraudulent marketing claims from the defendant's Internet Service Provider (ISP). Id. at 281. The defendant challenged such access to his email on Fourth Amendment grounds. Id. at 282. The Sixth Circuit agreed and held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" Id. at 288 (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)). In finding that a reasonable expectation of privacy existed in this case, the Sixth Circuit analogized email transmitted via ISP to the contents of telephone conversations and closed letters, each of which received Fourth Amendment protection. See id. at 286–87. Rebutting the third-party doctrine argument, the Sixth Circuit—similar to the SJC in Augustine above—noted that the ISP in this case was an *intermediary* rather than the intended target of a conversation. Id. at 288. Thus, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." Id. Though binding only in the Sixth Circuit, this case has been cited by some of the largest email providers in requiring warrants to obtain the contents of email. See Brendan Sasso, *Facebook, email providers say they require warrants for private data seizures*, The Hill (Jan. 25, 2013), http://thehill.com/policy/technology/279441-facebook-email-providers-require-warrant-for-private-data. The Department of Justice also requires its prosecutors nationwide to follow this holding.

(4) Surveillance in Public: Public View Principle, Mosaic Theory, and More

Under the "public view" principle, individuals generally do not have a reasonable expectation of privacy in items or places that they expose to the public. California v. Ciraolo, 476 U.S. 207, 213 (1986) ("[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares"). In particular, "the government, without… a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance." Augustine, 467 Mass. at 252. (Note that this principle as stated in Augustine is in some tension with the SJC's decision in Mora, as discussed below.)

Courts have limited the public view principle in "constitutionally sensitive" settings (epitomized by the home) where individuals have a strong expectation of privacy that society is prepared to recognize, especially where technology has enabled previously infeasible collection of information about the inside of a home via surveillance technology situated outside the home (i.e., in public). See Kyllo v. United States, 533 U.S. 27 (2001) (holding warrantless surveillance of heat levels inside a home using thermal-imaging equipment outside the home to be an unconstitutional search).

Recent developments suggest that courts are increasingly recognizing constitutional warrant requirements in more situations involving surveillance in public places, when such surveillance is particularly expansive and detailed, or implicates "constitutionally sensitive" domains such as the home. The SJC has recognized the "mosaic theory" or "aggregation principle for the technological surveillance of public conduct," under which "'the cumulative nature of… information collected [when collected over a long enough period] implicates a privacy interest on the part of the individual who is the target of the tracking,'" even when the individual activities or data points surveilled would not enjoy constitutional protection taken alone. Commonwealth v. McCarthy, 484 Mass.493, 503-04 (2020)(quoting Augustine, 467 Mass. at 253); see also Jones, 565 U.S. at 416 (Sotomayor, J., concurring).

- Commonwealth v. McCarthy, 484 Mass. 493 (2020). The Court considered the constitutionality of warrantless use of automatic license plate readers (ALPRs), which are "cameras combined with software that allows them to identify and 'read' license plates on passing vehicles." Id. at 494. Drawing on the "mosaic theory," the SJC stated that "[a] detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts," and noted that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." Id. at 504, 506. On the facts of the case, however, the SJC found no constitutional violation: "[T]he analysis should focus, ultimately, on the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance [at issue]. … [F]or this case, we consider the constitutional import of four cameras placed at two fixed locations… [and] conclude that the limited use of ALPRs in this case does not constitute a search within the meaning of either art. 14 or the Fourth Amendment." Id. at 506, 508,509.

Pole camera surveillance is a notable area where courts' approaches in applying the "public view" principle have been shifting recently, especially after Carpenter, 138 S. Ct. 2206, and Jones, 565 U.S. 400. While "[m]ost courts to have addressed pole camera surveillance have concluded that it does not infringe on any reasonable expectation of privacy" under the "public view" principle, "several courts have reassessed prolonged pole camera surveillance." Commonwealth v. Mora, 485 Mass. 360, 364-65 (2020) (citing as examples United States v. Vargas, No. CR-13-6025 (E.D. Wash. Dec. 15, 2014) (six weeks of pole camera surveillance was search); State v. Jones, 2017 S.D. 59 (2017) (two months was search); People v. Tafoya, 2019 COA 176 (Colo. App. 2019) (three months was search)). Mora is the most recent Massachusetts case on pole camera surveillance.

- Commonwealth v. Mora, 485 Mass. 360 (2020). Investigators installed pole cameras on public telephone and electric poles for the purpose of surveilling the defendants. Id. at 361. Most of the cameras were aimed at the homes of defendants or other individuals; one was aimed at a street that a defendant used to conduct his drug business. Id. at 362. The cameras had video but not audio recording capabilities, they could not view inside any residence, and they did not have infrared or night vision capabilities; however, investigators could remotely zoom and angle the cameras in real time. Id. The footage was stored in a searchable format that allowed officers to review previously-recorded events. Id. The SJC held that the pole camera surveillance of the defendants' homes was a warrantless search in violation of Article 14 of the Massachusetts Constitution. Id. at 370-76. Pole camera surveillance of public streets frequented by the defendants away from their homes was not subject to a warrant requirement, however, as defendants had no reasonable expectation of privacy in those locations. Id. at 369. The defendants' homes did not have fencing or other attempts to shield the residences from view, a fact that the court held immaterial to the constitutionality of surveillance. Id. at 366-67. The court noted that the Fourth Amendment might well require the same outcome, but declined to reach the federal constitutional question as the case could be resolved on state constitutional grounds. Id. at 361.

(5) Peer-to-Peer and Other Network File Sharing

The following cases illustrate when making data accessible to the public or certain networks via peer-to-peer file sharing techniques eliminates one's reasonable expectation of privacy.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Defendant was an instructor at a high school's electronics shop. Police officers remotely observed pirated movies and child pornography in an open share folder of a computer named Joester7437, which was connected to the school's network. Id. at 103–05. [Note: Joester7437 was later determined to belong to a student. Id. at 105.] While searching the school for Joester7437, the police found a computer/server named "Nightcrawler." Id. at 105. Nightcrawler's screen displayed an open share folder with the same pirated movie as was found on Joester7437. Id. "The source of the open share was Sinister, another unauthorized computer logged onto the high school's network." Id. The police found Sinister in the defendant's office, but that computer was password protected. Id. They seized Sinister "on probable cause to believe that it contained child pornography and copyrighted intellectual property." Id. They then received a search warrant for it based on an affidavit

alleging: (1) both shared folders (in Joester7437 and Sinister) had a copy of the same pirated movie, (2) Joester7437's open share folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 111. The defendant did not dispute that he had no reasonable expectation of privacy in files shared with the network. Id. at 107. Instead, the defendant argued that he did have a reasonable expectation of privacy in his *private* files and that there was no probable cause to search the private files for child pornography. Id. The Court held that the affidavit in support of the search warrant did not establish probable cause to believe that child pornography was located in the private files on the defendant's computer (Sinister). Id. at 111. The SJC noted: "None of these facts, even when considered together, provided a 'substantial basis' to believe that the defendant's private files contained child pornography." Id.

- Commonwealth v. Hay, 90 Mass. App. Ct. 1122 (2016) (unpublished). Defendant argued that the pre-warrant investigation was a "search" within the Fourth Amendment because the P2P [peer-to-peer] network was open only to a small group of known individuals, id. at *6, and because law enforcement used specialized SHA technology to identify a file on the defendant's computer that was likely to contain child pornography, id. at *7 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001) (government's use of device not in general public use "to explore details of the home that would previously have been unknowable without physical intrusion" is a search)). The appeals court held that, though it is possible that a file-sharing network open only to a small group of known individuals might give rise to a reasonable expectation of privacy in the files, the defendant had not argued or shown that the network in question here (Gnutella), as used with the specific software client used by the defendant (LimeWire), was such a network. Id. at *7. The appeals court also held the investigation was not a search because the defendant offered no evidence that the SHA technology enabled law enforcement to learn any more about the files than could any other P2P user. Id.

- United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010). Defendant shared child pornography over a peer-to-peer file sharing network that was being monitored by police using special forensic software. Id. at 1046–47. Police remotely downloaded the incriminating files from the defendant's folder on the peer-to-peer network. Id. at 1047. The Ninth Circuit held the defendant had no reasonable expectation of privacy in files that anyone who had access to the network could download. See id. at 1048. The court ruled this way notwithstanding the defendant's attempts to keep the files private because even though his subjective intent demonstrated a desire for privacy, it would be objectively unreasonable to uphold an expectation of privacy "in the face of such widespread public access." Id. The court also rejected the defendant's argument that the special forensic software used by investigators constituted a search. It cited several other cases supporting the proposition that special tools could be used to access already-public information, like the files in this case, because public information enjoys no Fourth Amendment protections. See id. at 1048.

- United States v. King, 509 F.3d 1338 (11th Cir. 2007). Defendant had child pornography on a personal computer connected to a military base network. Id. at 1339. His "files were 'shared' over

the entire base network," id. at 1342, and an airman searching the network remotely downloaded those files, id. at 1340–41. The defendant took several steps—ultimately unsuccessful—that he believed shielded his hard drive from access by others. Id. at 1341. Even though the defendant manifested a subjective expectation of privacy by attempting to secure the files, id., the court found that his failure to actually secure the files rendered that expectation objectively unreasonable, id. at 1342. In reaching this conclusion, the court analogized to a prior case holding that a defendant had no objectively reasonable expectation of privacy in the unsecured common area of a multi-unit apartment building. Id. In both cases, the fact of public access rendered any subjective expectation of privacy objectively unreasonable. Id.

- United States v. Ladeau, No. 09–40021–FDS, 2010 WL 1427523 (D. Mass. April 7, 2010). Defendant shared child pornography over a secured peer-to-peer network that allowed him to select who could download his files. Id. at *1. He allowed downloads by a private user who then turned his account over to the Royal Canadian Mounted Police. Id. The court held that even though the defendant manifested a subjective expectation of privacy through his actions, this expectation was not objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at *4. "No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access." Id. So, "[o]nce Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable." Id. at *5.

- United States v. Thomas, Nos. 5:12–cr–37, 5:12–cr–44, 5:12–cr–97, 2013 WL 6000484 (D. Vt. Nov. 8, 2013). Defendants in this case shared child pornography over peer-to-peer networks. Id. at *17. Police found the defendants by using automated scanning tools designed to detect child pornography shared on peer-to-peer networks. Id. After a lengthy explanation of file sharing, hash values, and investigative software and testing tools, id. at *2–6, the court held that the defendants had no reasonable expectation of privacy in files they shared publicly on a peer-to-peer network, id. at *19–20. In making this ruling, the court relied on United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010), along with other circuit cases. Id. at *19. The defendants argued against the inclusion of partially downloaded files in the evidence used against them, saying they would not have shared those files once the download was complete, but the court rejected this argument because those files were nonetheless being shared when the police searched and were therefore publicly accessible. Id. at *17. [Note: This case contains clear and thorough explanations of peer-to-peer networks, hash values, and TLO's CPS suite of tools.]

(6) Expectation of Privacy in Data That Is Not One's Own

The following cases address claims of a reasonable expectation of privacy in data that, in some sense, is not the movant's.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to

challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105,107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Almonor, the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Commonwealth v. Almonor, 482 Mass. 35, 47-48 (2019) (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The Court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Lugo, 482 Mass. at 108. During the investigation, police became concerned that a second juvenile involved in the murder-robbery might be in danger, and contacted that individual's cell phone service provider, obtaining location data, and the names and numbers from recent calls. Id. at 106. Among these was the defendant's phone number, which police also "pinged," showing that he was at his residence with the second juvenile. Id. Police obtained a search warrant for the residence and "discovered evidence linking the defendant to the killing, including the murder weapon." Id. The SJC pointed out that, even if there had been no standing issue, the circumstances of police investigating a homicide and concerned for the cell phone user's safety would have rendered the defendant's challenge futile under the emergency aid exception. Id. at 108. The Court also held that, while the defendant had standing to challenge the search of his own cell phone, the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 109.

- Commonwealth v. Bryant, 447 Mass. 494 (2006). Law enforcement seized the "main file server" of a law firm pursuant to a warrant. See Commonwealth's Brief, 2005 WL 4062684, at *10 (Dec. 2005). The defendant, an employee of the firm, moved to suppress files he had worked on. See Bryant, 447 Mass. at 495. Denying the motion to suppress, the Supreme Judicial Court held that the defendant did not have a "reasonable expectation of privacy" in the firm's files and therefore did "not establish[] that he ha[d] standing to challenge the seizure of the files." See id. at 497.

(7) Probationers, Parolees, and Court-Ordered Monitoring

Probationers subject to court-ordered monitoring have a diminished expectation of privacy.

- Commonwealth v. Feliz, 481 Mass. 689 (2019) (decided on the same day as Commonwealth v. Johnson, 481 Mass. 710 (2019), infra). The SJC held that Mass. Gen. Laws ch. 256, § 47, which mandates GPS monitoring as a condition of probation in connection with most sex offense convictions, is "overinclusive" because "GPS monitoring will not necessarily constitute a

reasonable search for all individuals convicted of a qualifying sex offense." Id. at *1; Mass. Gen. Laws ch. 256, § 47 (2018). The Court held that, under Article 14 of the Massachusetts Declaration of Rights, an individualized determination of reasonableness is required for any search that is "more than minimally invasive," and "GPS monitoring is not a minimally invasive search." 2019 WL at *7. Thus, a judge must "conduct a balancing test that weighs the Commonwealth's need to impose GPS monitoring against the privacy invasion occasioned by such monitoring." Id. at *1. Whether the monitoring is determined to be reasonable "depends on a constellation of factors," and "no one factor will be dispositive in every case." Id. at *8. The fact that a probationer accedes to a contract of probation that requires GPS monitoring or signs a GPS equipment contract does not constitute consent that waives the probationer's Article 14 rights. Id. at *8. With respect to Mr. Feliz, the SJC held that "the Commonwealth's particularized reasons for imposing GPS monitoring . . . do not outweigh the privacy intrusion occasioned by the requirement of GPS monitoring." Id. at *8; accord id. at *10–13. In support of that conclusion, the Court noted that the defendant "was convicted of noncontact sex offenses," and that the Commonwealth "ha[d] not presented evidence sufficient to indicate that th[e] defendant pose[d] a threat of reoffending or otherwise violating the terms of his probation." Id. at *10.

- Commonwealth v. Johnson, 481 Mass. 710 (2019) (decided on the same day as Commonwealth v. Feliz, supra). At defendant's trial for breaking and entering and larceny, the Commonwealth introduced GPS location data recorded from a GPS monitoring device that the defendant was wearing as a condition of probation. Id. at *1. The historical GPS data had been retrieved and reviewed without a warrant after the defendant's probation was completed. Id. at *2–3, *6. Defendant argued that the trial court erred in admitting the GPS location data at trial. Id. at *3. The SJC held that (1) the original imposition of GPS monitoring as a condition of defendant's probation was a search, but it was reasonable "in light of the defendant's extensive criminal history and willingness to recidivate while on probation"; and (2) no subsequent search occurred because, "once the GPS device was attached to the defendant, he did not possess a reasonable expectation of privacy in data targeted by police to determine his whereabouts at the times and locations of suspected criminal activity that occurred during the probationary period." Id. at *1. The SJC noted that the police had conducted a narrow analysis to determine whether the defendant was present at times and places where crimes had been committed, and that a broader "indiscriminate rummaging" through months of GPS data "might raise different, more difficult constitutional questions about objective expectations of privacy, even for a probationer subjected to GPS monitoring." Id. at *10.

- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017). Police investigating a robbery "mapped" the location of a defendant wearing a GPS monitoring device while out on bail for a domestic violence offense. See id. at 298. This process revealed that the defendant was near the scene of the robbery at the time of the break-in. See id. The Commonwealth introduced the GPS evidence at trial and the defendant was convicted. Id. at 296–97. The Massachusetts Appeals Court affirmed, rejecting defendant's argument that he—subject to court ordered monitoring—retained a reasonable expectation of privacy in his movements and thus was subject to a Fourth Amendment "search". See id. at 306.

Parolees have a diminished expectation of privacy—lower even than that of probationers—both under the Fourth Amendment, Samson v. California, 547 U.S. 843, 850 (2006), and under art. 14, Commonwealth v. Moore, 473 Mass. 481, 485 (2016). In Moore, the SJC determined that, "at least with respect to a search of the parolee's home," the reasonable suspicion standard associated with stop and frisk is the appropriate standard for a warrantless search. Id. at 487. Reasonable suspicion for the search of the home was supplied here by an anonymous tip that the parolee was dealing drugs, coupled with evidence of the parolee's conduct consistent with that tip in light of the parole officer's experience with narcotics and with other parolees. Id. at 490.

b) Seizures and Interference with Possessory Interest

Police actions reaching an individual's property constitute a seizure when "there is some meaningful interference with an individual's possessory interests in that property." Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (internal quotation marks omitted). As Justice Stevens noted in Texas v. Brown, 460 U.S. 730 (1983), "a seizure is usually preceded by a search, but when a container is involved the converse is often true . . . for example, the seizure of a locked suitcase does not necessarily compromise the secrecy of its contents . . . ." Id. at 747–48 (Stevens, J., concurring). Relying on ample precedent from other courts, the Supreme Judicial Court has found the entire computer analogous to such a closed container for seizure purposes. See Commonwealth v. McDermott, 448 Mass. 750, 766 (2007) (agreeing with lower-court "judge's analogy to closed containers with respect to the seizure of the computers and disks"). Whether a seizure has occurred is usually obvious and rarely contested. The following cases concern less-common circumstances.

- Berger v. New York, 388 U.S. 41 (1967). The Court held that wiretaps "seize" conversations in violation of the Fourth Amendment. Id. at 59. The Court did not expand further on how it came to this conclusion, but this case is often cited for the proposition that intangibles (e.g., data) can be seized in the constitutional sense. See, e.g., LeClair v. Hart, 800 F.2d 692, 695 (7th Cir. 1986) ("Following Berger, it has been clear that the Fourth Amendment embraces more than just the forced physical removal of tangible objects . . . . Indeed, Berger stands for the proposition that the government may seize intangible items, such as the information contained in the financial documents which the IRS agents copied.").

- Commonwealth v. Connolly, 454 Mass. 808 (2009). As part of an investigation of a suspected drug dealer, police installed a GPS tracking device in his car. Id. at 10. To install the device, police opened the car's engine compartment, placed the tracking device inside, and attached it to the car's battery. See id. at 812. The Supreme Judicial Court held that installing the GPS device was a seizure within the context of art. 14 of the Massachusetts Declaration of Rights. Id. at 822. First, the installation and presence of the tracker constituted a physical intrusion on the defendant's property. Id. Second, the government's use of the vehicle to obtain information was itself an interference with the defendant's interest in it. Id. at 823 ("It is a seizure not by virtue of the technology employed, but because the police use private property (the vehicle) to obtain information for their own purposes.").

- United States v. Hicks, 438 F. App'x 216 (4th Cir. 2011). Defendant destroyed his hard drive after he found out he was under investigation for possession of child pornography. Id. at 18. After he was convicted of destroying records in a federal investigation, the defendant attacked his conviction on constitutional grounds. Id. One of these challenges was that by criminalizing his destruction of his hard drive, the government had interfered with his possessory interest in that hard drive, effectively seizing it in violation of the Fourth Amendment. Id. at 219. The Fourth Circuit found that there was no meaningful interference with the defendant's possessory interest because he did not have a property right in images of child pornography. Id. (citing Helton v. Hunt, 330 F.3d 242, 247 (4th Cir. 2003), for the proposition that there is no property right in contraband).

The case summarized below discusses the return of unlawfully seized property:

- Commonwealth v. Salmons, 96 Mass. App. Ct. 61 (2019). The defendant pled guilty to assault and battery by means of a dangerous weapon, intimidating a witness, strangulation, and other charges. The police had seized the defendant's three cell phones at the time of arrest, but the seizure was subsequently found unlawful based on the SJC's decision in Commonwealth v. White, 475 Mass. 583 (2016) (probable cause to seize or search a cell phone requires "information establishing the existence of particularized evidence likely to be found there," id. at 593). Salmons, 96 Mass. App. Ct. at 62. The defendant filed a motion for the return of his cell phones, which was granted. Id. at 62. Eight months later, the Commonwealth moved to wipe the content of two of the phones before returning them, because they contained "numerous and sexually explicit photographs and videos of the defendant and [the victim]." Id. The motion to wipe these phones was allowed, id. at 65, but the Appeals Court reversed. Relying on Commonwealth v. Sacco, 401 Mass. 204 (1987), the Court found that "when, as here, property is unlawfully seized without a warrant, cannot be used as evidence, and is not unlawful to possess, it should be returned, upon proper motion, to its undisputed owner or the owner's representative." Salmons, 96 Mass. App. Ct. at 68. There was no factual finding that harm to the victim would occur unless the phones were wiped. Id. at 69. Further, the Commonwealth's reliance on Beldotti v. Commonwealth, 41 Mass. App. Ct. 185 (1997) was misplaced because the public interest standard of G.L. c. 276, § 3 did not apply to property seized unlawfully and because the "connection between the crime and the property here [was] far more attenuated than in [Beldotti]." Id. at 69-70.

c) Private Party Searches

(1) Initial Search Made by Private Party

"[W]hen the state conducts a search in response to information that a private party obtained and communicated to the government, 'the legality of the governmental search must be tested by the scope of the antecedent private search.'" Commonwealth v. Cormier, 28 Mass. L. Rptr. 489, at *4 (Mass. Super. Ct. 2011) (quoting United States v. Jacobsen, 466 U.S. 109, 116 (1984)). Where the government searches something in which a private party has already eroded a suspect's expectation of privacy, the Fourth Amendment is not implicated. Id. (citing Jacobsen, 466 U.S. at 116). Crucially, police examination of

materials "initially discovered and viewed by a private party" can be more thorough than that private party's examination and still fall within the scope of the private party search. Id. at *5 (citing Commonwealth v. Raboin, 24 Mass. L. Rptr. 278, 282–83 (Mass. Super. Ct. 2008)). A more detailed analysis of Commonwealth v. Cormier below demonstrates how the private party search doctrine applies to digital evidence cases.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. at *2. Police found more child pornography at the defendant's house, and he was later charged with possession. Id. The trial judge denied defendant's motion to suppress because the warrantless search conducted by police was within the scope of the preceding private party search. Id. at *4–6. Because the computer technician had previously viewed files from the hard drive, the court found that the defendant's expectation of privacy "had already been eroded," so the subsequent police search did not implicate the Fourth Amendment. Id. at *5.

(2) Warrantless Search: Private Citizen or State Actor

If the intent of a private party conducting a search is not independent of the government's intent, however, the private party becomes an agent of the government, implicating the Fourth Amendment and art. 14. See Commonwealth v. Leone, 386 Mass. 329, 333 (1982). A party becomes a state actor if the police do anything to "solicit, provoke, or tempt" that party into obtaining evidence for them. Commonwealth v. Brandwein, 435 Mass. 623, 631 (2002). The cases below examine the state actor issue in the digital evidence context.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. The court found that the data recovery shop employee was not acting as a state agent because he was a private party not acting under the authority of the state. Id. at *4 (citing Commonwealth v. Leone, 386 Mass. 329, 333 (1982), for the proposition that "[e]vidence discovered and seized by private parties is admissible without regard to the methods used, unless State officials have instigated or participated in the search"). The court noted that the employee "made the decision to open the suspicious files . . . as a private citizen, while trying to repair the hard drive at [defendant's] request." Id. The court also found that authorities "did not know that [the defendant] asked [the employee] to repair his hard drive and did not instruct [the employee] to inspect the files." Id. They did nothing "to 'solicit, provoke, or tempt' [the employee] into viewing the files," so he was not a state actor. Id. (quoting Brandwein, 435 Mass. at 631).

- United States v. Lichtenberger, 19 F. Supp. 3d 753 (N.D. Ohio 2014). A private party called police after discovering child pornography on a computer, and the responding officer instructed that individual to boot up the laptop, enter the password, show the images, and gather other devices belonging to the defendant before seeking a warrant. Id. at 754–55. The court found these actions violated the Fourth Amendment because by giving instructions and directing the private party's actions, the police officer made that private party into a government agent. Id. at 758–59. The court therefore suppressed the evidence as having been collected in violation of the Fourth Amendment. Id. at 760.

(3) An ISP's Reporting Obligation Does Not Make it a State Agent

The reporting requirement of 18 U.S.C. §§ 2258A(a) and 2258B(a)—requiring an Internet service provider (ISP) to report any child pornography that it discovers—does not transform an ISP into a government agent when it chooses, voluntarily, to scan files sent on its network for child pornography. United States v. Stevenson, 727 F.3d 826, 829–30 (8th Cir. 2013).

2. Was a Search or Seizure Reasonable?

"The ordinary rule is that to be reasonable under the [Fourth] Amendment a search [or seizure] must be authorized by warrant issued by a magistrate upon a showing of probable cause." Almeida-Sanchez v. United States, 413 U.S. 266, 287 (1973); see also United States v. Carpenter, 138 S. Ct. 2206, 2221 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.") (quoting Riley, 134 S. Ct. at 2482)). This section will lay out the requirements of a valid warrant in the cybercrime context and then highlight some applicable exceptions to the warrant requirement.

a) Warrants

"The Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights require that a warrant be issued only on probable cause, supported by oath or affirmation." Commonwealth v. Nelson, 460 Mass. 564, 568 (2011). Massachusetts law specifically "require[s] an affidavit and an oath." Id. (citing Mass. Gen. Laws ch. 276, §§ 1 and 2B). A neutral magistrate must issue the warrant, see Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971), and it must be particular as to the items to be seized and places to be searched, see Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Warrants must contain information that has not been rendered stale, see United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (to evaluate staleness, courts "must assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information"). In addition, officers must execute warrants in a timely fashion, see Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 329–30 (2014) ("[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event no later than seven days from the date of issuance thereof." (quoting Mass. Gen. Laws c. 276, § 3A)). Warrants must be executed in a reasonable manner. Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). Finally, executing officers must have the signed

warrant with them when commencing the search. The sections below focus on probable cause, particularity, staleness, timely execution, and the manner of executing warrants in the digital evidence context.

(1) Probable Cause / Affidavit

"Under the Fourth Amendment and art. 14, probable cause requires a substantial basis for concluding that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues." Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009) (internal quotation marks and citations omitted) (detailed below). Further:

> The affidavit need not convince the magistrate beyond a reasonable doubt, but must provide a substantial basis for concluding that evidence connected to the crime will be found on the specified premises. Moreover, affidavits for search warrants should be interpreted in a commonsense and realistic fashion and read as a whole, not parsed, severed, and subjected to hypercritical analysis. All reasonable inferences which may be drawn from the information in the affidavit may also be considered as to whether probable cause has been established.

Commonwealth v. Donahue, 430 Mass. 710, 712 (2000) (internal quotation marks and citations omitted).

In order to establish probable cause, law enforcement officials must typically submit an affidavit to a magistrate. That magistrate's probable cause determination is confined to the "four corners" of the affidavit. Commonwealth v. Anthony, 451 Mass. 59, 68 (2008) (detailed below). Probable cause by definition deals with "probabilities," which "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Id. (internal quotation marks and citations omitted). The following cases address probable cause and affidavits in the digital evidence context.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. The warrant affidavit "provided a substantial basis to conclude both that the defendant had committed the homicide [with a] coventurer and that it was reasonable to expect that his cell phone would contain evidence related to that specific crime." Id. at 587. Here, unlike in Commonwealth v. White, 475 Mass. 583 (2016), there was specific evidence of a nexus between the crime and the defendant's cell phone. Id. at 589. This evidence included the following facts: "the defendant made a cell phone call soon after the shooting to the person who rented the car used in the murder, there [was] a reasonable inference that the crime was

preplanned, and there [were] records of threatening cell phone communications between [the defendant's [coventurer] and the victim." Id.

- Commonwealth v. Vasquez, 482 Mass. 850 (2019). The defendant was indicted on charges of murder in the first degree and two related firearms offenses. He moved to suppress witnesses' identification of him from surveillance footage, his statements to the police, as well as evidence obtained from the search of his phone and the CSLI. Id. at 851. The SJC found that the witness identification did not require suppression. But the SJC agreed with the trial court's finding that the Miranda warnings were rendered in Spanish "in such a fragmented and confusing manner so as to be incoherent." Id. at 862. More specifically, the improper translation rendered the warnings "inadequate to apprise the defendant of his rights, and [ ] the defendant's limited comprehension of English did not suffice to compensate for these deficiencies." Id. at 852. Because the Miranda warnings were insufficient and the search of the defendant's cell phone arose from the statements the defendant made after the defective warnings, the search was not sufficiently attenuated from the unwarned statements. Id. at 865. Further, without the tainted information from the unwarned statements (such as the defendant's disclosure of his phone number), the Commonwealth failed to establish "the requisite nexus between the commission of [the] crime and the CSLI for the defendant's device." Id. at 867. The Commonwealth also failed to establish a connection between the crime and the thirty-two days for which it sought CSLI. Id. In sum, the search warrant affidavit did not "support a determination of probable cause, and the CSLI obtained as a result must be suppressed." Id. at 868. The SJC remarked in a footnote, however, that CSLI evidence may be admissible later, if the Commonwealth could show by a preponderance of the evidence that there was an untainted source for the nexus between the crime and CSLI. Id. at 868 n. 27 (quoting Commonwealth v. Estabrook, 472 Mass. 852, 865 (2015)).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). Following conviction for first-degree murder, the defendant argued on appeal, among other things, that the motion judge erred in denying his pre-trial motion to suppress cell site location information (CSLI) that was introduced as evidence during his trial. Id. at 539. The defendant's brother had identified the defendant as the man leaving the crime scene in video footage, and provided police with a phone number he claimed belonged to the defendant. Id. at 541. Police then requested a court order requiring the service provider to produce CSLI from the cell phone for several months surrounding the day of the crime. Id. at 541. The CSLI placed the owner of the cell phone in the general vicinity of the crime at the time of the killing. Id. The Court ruled that, although it was a close call, the police affidavit in support of a search warrant for historical CSLI satisfied the requirement that "there be a substantial basis to believe that the sought-after CSLI 'will produce evidence of [the] offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed . . . such offense.'" Id. at 545-46 (quoting Commonwealth v. Augustine, 472 Mass. 448, 453 (2015)). The Court rejected the defendant's assertion that the police must demonstrate that the cell phone was used or possessed during the commission of a crime in order to show nexus between "the crime . . . the items sought, and the location to be searched." Id. at 546. This is not necessary because "[c]ell phones physically accompany their users everywhere such that tracking a cell phone results in near perfect surveillance of its user." Id. at 547 (quoting

Commonwealth v. Almonor, 482 Mass. 35, 45 (2019) (internal quotation marks omitted)). The defendant's brother's statement that the cell phone belonged to the defendant, together with subsequent corroboration by the defendant's former girlfriend, was enough to establish the requisite nexus. Id. at 548-49.

- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019). The indictments in this case alleged that the defendant and two co-conspirators broke into the defendant's uncle's home and beat him on the head and face with a crowbar. Id. at 618. The defendant was charged with home invasion, assault, and multiple other offenses. Id. at 618, n. 1. She moved to suppress the fruits of a search of her cell phone. The Superior Court allowed the motion, but the Appeals Court reversed, finding that the police had probable cause to seize the phone, and that the defendant voluntarily consented to an unlimited search of her phone. There was probable cause to seize the cell phone because the defendant told the police it contained videos that "could establish where, when, and with whom the defendant was in the hours before the home invasion." Id. at 623. The police were also aware of multiple facts connecting the defendant to the crime. For example, her car was seen near the victim's home less than two hours before the assault, she had a key to the victim's residence and there was no sign of forced entry, the victim had a restraining order against the defendant, and there were blood stains in the exterior of the defendant's car. Id. In sum, the seizure was lawful because the police had "a substantial basis for concluding" that the phone contained "evidence connected to the crime under investigation." Id. The court also ruled that the defendant's subsequent "consent to search her cell phone was without limitation." Id. at 625-26. The police communicated their intent to search the entire cell phone to the defendant, and she consented to the search, providing the police with passwords to the phone and to her Snapchat account. Id. at 626. Applying "a common sense interpretation" to the defendant's entire exchange with the police detective, the Appeals Court found that her "consent to search her cell phone was free, voluntary, and unlimited." Id.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police approached the defendant sleeping in the stairwell and seized a cell phone on the floor nearby. Id. at 282. There was probable cause to seize the phone because the police "had information that the defendant and victim had been together on the day of the murder, and also that [the murder victim's boyfriend] had recently overheard the defendant confessing to the murder to an unidentified person on a cell phone." Id.

- Commonwealth v. Martinez, 476 Mass. 410 (2017). State police used law enforcement version of P2P client to investigate sharing of child pornography, identified such activity coming from a Massachusetts IP address, and subpoenaed Comcast for information regarding the IP address for the 30-minute period on March 9, 2012, during which police downloaded four suspected child pornography video files shared from the account associated with the IP address. Id. at 411–13. The ISP gave police a name (Angel Martinez) and an address. Id. at 413. Local law enforcement then obtained a warrant to search the apartment located at the address for computers and related items connected to the suspected possession and distribution of child pornography. Id. The apartment was leased to the grandmother of the Comcast account holder and of the defendant (Adalberto Martinez). Id. at 413 n.2. Law enforcement seized two laptops belonging to the

defendant and found five videos containing child pornography on one of them. Id. The SJC held that the affidavit in support of the search warrant (containing information that a particular IP address was used to share child pornography and that this IP address had been assigned at the time to a subscriber at the specific physical address to be searched) was sufficient to establish probable cause for the search, even though the named subscriber was neither listed as, nor confirmed to be, living in the apartment searched, and even though police had no information before the search linking the defendant to the residence. According to the SJC, law enforcement did not have to verify that the account holder lived at the address searched. Id. at 418. Once the nexus between the crime and the service address was established, the names of the account holder and of the leaseholder were incidental. Id. The SJC rejected the argument that law enforcement had to show that the network was secure or that no one outside the address could access the network. Id. at 419. Where the warrant was for the search of a place (not for the arrest of a person), law enforcement needed only demonstrate a sufficient nexus between the criminal activity under investigation, the items sought, and a place to be searched. Id. Even assuming law enforcement could know a network was not secured, unauthorized use of the network did not negate the substantial basis to think the evidence would be located at the address. Id. at 420–21 ("[P]robable cause does not require investigators to 'establish to a certainty that the items to be seized will be found in the specified location,' nor does it require them to 'exclude any and all possibility that the items might be found elsewhere.'" (quoting Anthony, 451 Mass. at 70)).

The decision came with caveats. The SJC cautioned that its decision here does not mean that probable cause always exists any time investigators link illegal computer activity to an IP address and then link that IP address to a physical address. Martinez, 476 Mass. at 422. To support probable cause, law enforcement should use reliable methods—such as the administrative subpoena here—to connect the IP with a physical address, not IP address mapping services. Id. at 423. Additionally, some technologies (e.g., Tor exit relays, VPNs, and proxy server connections, which can mask originating IP addresses) may erode the connection between an IP and a physical address. Id. Law enforcement may be required to disclose in affidavits the possibility that one of these technologies was, or may have been, used based on facts known or reasonably knowable to investigators at the time. Id. "If such technologies become more common, it is entirely possible that we would require police to proceed in multiple steps, obtaining subpoenas related to each intermediary IP address or warrants to search each location hosting those IP addresses." Id. In some cases, law enforcement may be required to determine, by forensic examination of a wireless router, which devices were connected to it and when before searching particular computers. Id.

- Commonwealth v. Perkins, 478 Mass. 97 (2017). "Based on intercepted telephone conversations between defendant's alleged middleman and street-level distributor of cocaine, police surveillance of suspected drug transaction, and other information, the judge issued a warrant authorizing a search of the defendant's apartment for evidence including a cellular telephone and drug-related records." Id. at 99. The warrant also included authorization to seize currency, distribution paraphernalia, documentation about the premises and its contents, among other items. Id. at 101. The affidavit did not seek authorization to search for narcotics. Id. at 98. Police seized a large quantity of cocaine, several cell phones, drug paraphernalia, and ammunition. Id. at 101.

The SJC concluded that the affidavit justified searching the apartment for the defendant's phone. Id. at 105–06. They further concluded that the seizure of nine additional phones found in the apartment was supported by probable cause, but that the police did not have discretion to "search every portion" of these additional phones. Id. At 106. Instead, the plain terms of the warrant restricted their search to call activity and contact lists and did not authorize police to "rummage through the entirety of the defendant's cellular telephones." *Id*. At 106. With regards to searching the defendant's apartment for records, proceeds, and paraphernalia, however, the SJC held that the affidavit:

> did not contain sufficient particularized information to justify [such] a search of the defendant[']s apartment . . . . The affidavit included a single, conclusory statement that probable cause existed based on the affiant's "training and experience and the facts and circumstances learned during the course of this investigation," [but] contained no facts, or opinion based upon the affiant's considerable experience as a narcotics officer, that would have establish[ed] probable cause to believe that the defendant would be likely to store particular items of [drug-related records, proceeds, or paraphernalia] in his home.

Id. at 109.

- Commonwealth v. Jordan, 91 Mass. App. Ct. 743 (2017). In a murder investigation in which defendant was a suspect, police obtained search warrant for his CSLI, call details, text messages, and subscriber information for a six-week period surrounding the date of the homicide. Id. at 744. The Appeals Court found that the trial judge properly suppressed the text messages. Id. Although the affidavit in support of the warrant established probable cause to believe that the victim had been murdered (i.e., a crime had been committed), it made no connection between the defendant's use of his cell phone and his involvement in the crime, and thus did not establish probable cause to conclude that the text messages would provide evidence connected to the crime. Id. at 749–51. The affidavit did establish probable cause to conclude that the defendant committed the crime and showed that the defendant had a cell phone and that it was in use around the time of the murder, and so it established probable cause to believe that the CSLI would provide evidence of the defendant's involvement in the crime. Id. at 750–53. The SJC also held that the trial court had properly suppressed "contact information" insofar as that meant an address book or contact list because the affidavit failed to establish a nexus between the crime and the defendant's contact information. Id. at 753–54. However, if "contact information" meant subscriber information and call records, there was no basis for suppression. Id.

- Commonwealth v. Keown, 478 Mass. 232 (2017). Defendant was suspected of murdering his wife by poisoning her. In the course of the investigation, police obtained a warrant to search his computer and discovered evidence of incriminating Internet searches, which was introduced at trial. Id. at 234–37. The SJC held the affidavit established a sufficient nexus between the crime and the item sought where: (1) it established the defendant's sophistication with computers (he had worked as a Web designer), and showed that he had forged contracts and admissions letter/other communications from Harvard Business School (can infer he used computer); (2) it described forgeries related to the motive alleged in the affidavit, i.e., to kill his wife to prevent her

finding out about their impending financial ruin and his lies and to collect her life insurance benefits; (3) it specified that the victim had died from ethylene glycol poisoning which, the affiant noted, would likely have involved online research. Id. at 238–39.

- Commonwealth v. Broom, 474 Mass. 486 (2016). At the time of defendant's arrest for murder, his cell phone was seized. Id. at 494. Ten months later, law enforcement applied for and obtained a search warrant for its contents. Id. The affidavit contained information about the investigation and the fact that no CSLI information could be obtained for the time surrounding the murder but that the defendant's phone records showed he sent and received text messages and accessed the Internet at the relevant timeframe. Id. It then described the many types of data the detective wanted to search in order to uncover information pertinent to the investigation. Id. at 494–95. The SJC held the search was not supported by probable cause. Id. The Court held that "it is not enough that the object of the search *may* be found in the place subject to search. Rather, the affidavit must demonstrate that there is a reasonable expectation that the items sought *will* be located in the particular data file or other specifically identified electronic location that is to be searched." Id. at 496 (citations omitted) (emphasis in original). Police here already had the defendant's CSLI (except for the time period surrounding the murder) and call records and would have known that the victim's number did not appear in those records. Id. The warrant was also found to be too broad. Id. at 495, 496 n.13.

- Commonwealth v. White, 475 Mass. 583 (2016). A police investigation of an armed robbery and shooting led to the defendant as one of three suspects. Id. at 584. After suspicion focused on him, the detective located his phone, which was held by the defendant's school administrator pursuant to school policy. Id. The detective then "seized the telephone to prevent the defendant from retrieving it and removing evidence or destroying the device." Id. Police had no information at the time indicating that the phone had been used to plan, commit, or cover up the armed robbery they were investigating, or that it contained any evidence of the crime, but instead relied on knowledge that cell phones are frequently used when the offense involves multiple perpetrators. Id. Sixty-eight days after the seizure, police obtained a warrant to search the cell phone and found evidence that was later ordered suppressed. Id. The SJC held that the seizure was not supported by probable cause because probable cause may not be based solely on an officer's opinion that the device is likely to contain evidence of the crime under investigation. Id. at 584–85. "[E]ven where there is probable cause to suspect the defendant of a crime, police may not seize or search his or her cellular telephone to look for evidence unless they have information establishing the existence of particularized evidence likely to be found there." Id. at 590–91. A contrary decision would mean that, where probable cause to charge someone with a crime existed, the person's phone would almost always be subject to seizure and subsequent search. Id. at 591.

- Commonwealth v. Williams, 90 Mass. App. Ct. 1118 (2016) (unpublished). The victim was shot after a drug deal with two suspects. Id. at *1–2. Two witnesses testified that the victim had arranged the deal via phone. Id. Police zeroed in on an 857 (area code) number linked to a person named Patrick Malone. Id. Defendant was then identified as the second suspect and was interviewed by police; he stated that he had known Malone for twenty years and that they had a

phone conversation on the morning of the shooting. Id. at *3–4. Police seized the defendant's iPhone and secured it to get a warrant. Id. The Appeals Court held that "there was probable cause to believe that the defendant's iPhone would contain evidence linking his alleged coventurer Malone to the 857 number and thus to the shooting." Id. at *5. See also Commonwealth v. Perkins, 478 Mass. 97, 105–06 (2017), (where police had detailed and specific knowledge about the defendant's use of a cell phone to arrange drug transactions, and a particular phone number with which that cell phone had been in contact at a specific time, there was probable cause to believe that the defendant used a cell phone to arrange a drug sale and that he had done so on other occasions and the seizure of nine cell phones from his apartment was proper). But see Commonwealth v. Fulgiam, 477 Mass. 20, 34 (2017) (where warrant application established a personal relationship between defendant and victim and the circumstances of the murders suggested a connection to drugs, it did not, without more, justify intrusion into the content of the communications between defendant and victim).

- Commonwealth v. Finglas, 81 Mass. App. Ct. 1102 (2011) (unpublished). Police were sent information about the defendant, whose email address had received five images depicting child pornography. Id. at *1–2. On interlocutory appeal, the Appeals Court granted the defendant's motion to suppress evidence obtained as a result of a search of his residence. Id. at *3. It did so because the affidavit in support of the warrant was "inadequate to establish a timely nexus between the defendant and the location to be searched and to permit the determination that the particular items of criminal activity sought reasonably could be expected to be found there." Id. The Appeals Court held that the affidavit did not provide any evidence that a computer at the residence had been used to search for or download any child pornography or that the defendant had actually accessed the emailed images. Id. at *2. Further, a police officer's opinion about the common practices of child pornography collectors was not enough, without further facts, to support a finding that the defendant's computer likely contained child pornography. Id. at 3.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it based on an affidavit alleging: (1) both shared folders had a copy of the same pirated movie, (2) the second computer's shared folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 105, 107–09. The Court invalidated the search warrant because it found police did not provide a "substantial basis" to believe there would be child pornography on the computer. Id. at 111. The Court found it unreasonable to infer that somebody interested in sharing a commercial movie would also be interested in sharing child pornography. Id. at 112. That the defendant had access to child pornography did not help the Commonwealth's case. Id. Nor was a suspicious statement, standing alone, enough to provide the substantial basis necessary for probable cause. Id. at 113.

- Commonwealth v. Anthony, 451 Mass. 59 (2008). Police received a tip about a person soliciting child pornography online. Id. at 60–62. They traced these solicitations to a library and arrested a

homeless suspect there. Id. at 62–63. Shortly after the arrest, the suspect took a receipt (along with other pieces of paper) out of his pocket and tore it up. Id. at 63. This receipt was from a repair shop for the repair of two laptops. Id. Police also determined he rented a storage locker. Id. at 64. Police sought and received a search warrant for the locker, the laptops, and a hard drive from the library. Id. at 65–66. A superior court judge granted the defendant's motion to suppress for lack of probable cause, however, and the Commonwealth pursued an interlocutory appeal. Id. at 67–68. The SJC reversed the motion judge's suppression of the warrant, finding the affidavit established probable cause. Id. at 73. Specifically, the Court found information about the suspect's prior conviction for child pornography, the outside tip, and the suspect's admission to viewing child pornography in violation of his probation established probable cause for the crime. Id. at 70–71. From there, it found the fact that a homeless individual rented a storage locker using a false address—along with the detective's experience that viewers of child pornography tend to collect it—supported the idea that the suspect might hide child pornography at his storage locker, the only space under his control. Id. at 71–72. The Court found the suspect tearing up the receipt supported the inference that he was trying to hide child pornography. Id. at 71. It emphasized that the affidavit did not rely solely on the opinions of the affiant with respect to general characteristics of collectors of child pornography. Id. at 72. Rather, the affidavit contained enough facts and inferences to support a nexus between the alleged crime and the locations to be searched. Id. 72–73.

(2) Independent Source Doctrine

- Commonwealth v. Wilson, 486 Mass. 328 (2020). The police initially obtained defendant's CSLI data pursuant to an § 2703 order, without a warrant, in 2010. Id. at 336. The CSLI placed the defendant in "the victim's hotel, at the commuter lot where the [victim's] rental vehicle was found, and in the location where the victim's body would later be discovered, at relevant times on the night of the murder." Id. at 331. In 2014, the police obtained the same CSLI information pursuant to a search warrant. The Court found that the 2014 warrant satisfied the "independent source doctrine," "a well-recognized exception to the exclusionary rule under both the Fourth Amendment and art. 14." Id. at 335. The doctrine provides that "evidence initially discovered as a consequence of an unlawful search may be admissible if later acquired independently by lawful means untainted by the initial illegality." Id. (quoting Commonwealth v. DeJesus, 439 Mass. 616, 624 (2003)). Here, the affidavit supporting the 2014 warrant for the CSLI was based on facts wholly independent of the CSLI data obtained in 2010. Id. at 336. These facts included the following: the defendant's public statements about having a firearm like the one used in the murder, his status as the likely father of the victim's unborn child, causing financial obligations to the victim and the "ire of the defendant's wife," the victim's statement to a friend that the defendant asked her to get an abortion, the cellphone communications between the defendant and the victim until shortly before the victim's cellphone activity ceased at 10:49 P.M. on the night of the murder, and a Facebook message from the victim's account after she was reported missing "claiming she was in the hospital after an abortion, although police determined that she was not a patient at any area hospitals." Id. at 337.

- Commonwealth v. Gosselin, 486 Mass. 256 (2020). The defendant appealed his conviction for first-degree murder, arguing, *inter alia*, that his trial counsel was ineffective for not moving to

suppress CSLI evidence, as such evidence provided probable cause for the search warrant for his home—the search of which produced critical inculpatory evidence. Id. at 264. The Court declined to resolve whether the § 2703 warrant was supported by probable cause, on the grounds that "the search warrant affidavit satisfied probable cause when excising the unconstitutionally obtained CSLI," such that the defendant failed to demonstrate prejudice and his trial counsel was not ineffective. Id. at 264-66 & n.9.

(3) Particularity / Scope

The Fourth Amendment, art. 14, and Mass. Gen. Laws ch. 276, § 2 all require that search warrant applications particularly describe the places to be searched and the items to be seized. See Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Massachusetts courts treat these provisions as coextensive. Id. The dual purpose of these requirements is (1) to protect people from general searches and (2) to provide the Commonwealth the opportunity to demonstrate to a court that officers' search authorization was properly limited. Id. Additionally, the requirement provides essential information to a person whose property is being searched. Id. (citing Katz v. United States, 389 U.S. 347, 356 (1967)). The cases below explore the tension between the particularity requirement and the amorphous nature of data in the digital era.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. However, the Court concluded "that the search of the phone was not sufficiently particular because it lacked any temporal limit." Id. at 583. More specifically, the Court held "that (1) the correct remedy for the warrant lacking particularity in this case [was] partial suppression; (2) the search of text messages, call logs, and Snapchat video recordings was proper; yet (3) the lack of time restriction rendered the warrant impermissibly broad." Id. at 590. Accordingly, the SJC remanded the case to the Superior Court to determine whether "the proffered evidence fell outside what would have been a reasonable temporal limit." Id. First, as to partial suppression, the Court noted "that an overbroad warrant generally requires only partial suppression of the information for which there was not the requisite nexus, as long as the Commonwealth had not relied on or otherwise exploited it at trial. Id. at 591-92 (quotations and citations omitted). Second, because the police here had probable cause to search the defendant's cell phone for evidence of joint venture, the scope of the search properly included communications such as call logs, text messages, and Snapchat videos. Id. at 593. Third, a cell phone search warrant cannot be sufficiently particular without some temporal restriction that should "err on the side of narrowness." Id. at 594. Where the initial search provides probable cause to broaden the search, "nothing precludes" officers from requesting another, broader warrant. Id.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case involving partial suppression of CSLI, the government requested 48 hours of a shooting suspect's CSLI around the time of the shooting, received 34 hours of CSLI in response to this request, and then had all but

three hours of CSLI ("covering the period approximately ninety minutes before and ninety minutes after the shooting") suppressed by the trial judge. Id. at 164. The SJC upheld this partial suppression of CSLI data, but noted in dicta that the "severance doctrine [of Hobbs] is not without limits," and that "where a warrant so lacks particularity or is so overbroad that it begins to resemble a general warrant, total suppression is required." Id. at 168-69. The court deemed the CSLI request at issue "not so overbroad on the facts of this case so as to be akin to a general warrant" and found it to "represent 'a reasonable period of time encompassing the commission of and flight from the crime.'" Id. at 169 (quoting Hobbs, 482 Mass. at 550). However, the SJC declined to provide further guidance on exactly "how overbroad a request for CSLI must be in order for total suppression to be appropriate." Id.

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). The government requested three and a half months of historical CSLI from defendant's cell service provider, from December 1, 2010 to March 15, 2011, where defendant was a suspect in a December 16, 2010 killing. Id. at 543, 550. "This extended request was in part the result of the failure to identify the defendant as a suspect for nearly two and one-half months, and the absence of any evidence of his current location once he was identified as a suspect." Id. at 550. The SJC considered the question of whether "either the Fourth Amendment or art. 14 require[s] total suppression of the entire amount of CSLI collected," or whether "the proper remedy [is] to suppress only the CSLI for which there is not the requisite nexus to the crime," and concluded that "where the requisite nexus for probable cause clearly exists for a reasonable period of time" contained within the requested period, "the CSLI for [the relevant] period of time need not be suppressed so long as the CSLI for which there is not the requisite nexus to the crime is not relied on or otherwise exploited by the Commonwealth at trial." Id. However, the court suggested its holding was fairly narrow, noting that "[g]iven the uncertainty in the case law regarding overbroad requests for CSLI, we proceed cautiously on this issue." Id. The Court also "emphasized the significant constitutional issues raised by the collection of extended amounts of historical CSLI, and the importance of limiting the requests accordingly." Id. at 550 n.13.

- Commonwealth v. Holley, 478 Mass. 508 (2017). In a murder investigation, law enforcement examined the victim's call records and learned that the last call the victim answered before the shooting came from the defendant's telephone number. Id. at 511. Law enforcement then obtained cell phone records through a warrant served on the carrier and found multiple incriminating communications via text and call between the victim and the defendant's joint venturer. Id. The warrant for the phone records sought "subscriber information; billing records and detailed airtime; outbound call detail; call origination and termination location; stored GPS location information, and/or stored cellular tower records, cell tower sector information, range from cell tower information (RTT) and physical address of cell sites; and all stored contents of electronic or wire communications including stored or deleted voicemail, read, unread, deleted, or sent electronic mail or text messages, and stored files; and listing of all associated phone numbers, of a subscriber to or customer of such service" between October 1 and 18, 2012. Id. at 524–25. The broad scope of the search raised "significant concerns" for the SJC because it did not sufficiently limit the scope of the search so as to prevent "exploratory rummaging." Id. at 525,

528. But because the record was silent on how the provider conducted the search and on what information, if any, it provided to the Commonwealth beyond the text messages (it was even unclear whether the provider kept any stored content apart from text messages as part of its business records) and because the only communications used at trial were the defendants' redacted text messages from four and two days before the shooting, respectively, the day of the shooting, and the day after the shooting, the Court could find no error in the denial of the motions to suppress. Id. at 525 (noting that the "Commonwealth did not capitalize on the lack of particularity in the warrant").

- Commonwealth v. Molina, 476 Mass. 388 (2017). Police investigating a P2P network found child pornography shared by a Massachusetts IP address. They subpoenaed Verizon and obtained a name (Hermes Delcid) and service address. Id. at 390–91. Further investigation found the name on the mailbox outside of the address and RMV records showed Delcid at the address. Id. at 391. Police then obtained a search warrant for the apartment and in particular for electronic devices containing evidence of child pornography, evidence of child pornography in other formats, evidence related to access to the Verizon account and the P2P network, and evidence related to access to electronic devices at the apartment. Id. In a bedroom later identified as the defendant's, police observed the P2P program running on an open laptop (computer screen showed downloads and uploads of child pornography files in progress). Id. at 392. The search team seized numerous electronic devices from the apartment, including the defendant's laptop and desktop computers and his external hard drive. Id. On appeal, the defendant argued that the search warrant was impermissibly overbroad as to both places and "things" to be searched. Id. at 393. The SJC disagreed. Id. at 389. It found that the warrant appropriately substantiated a connection between the apartment and the evidence of child pornography reasonably expected to be located therein. Id. at 394. That the apartment was shared by multiple people was immaterial because the warrant authorized a search of the location associated with the IP address, not a search of any single associated subscriber. Id. at 395. Computer devices using the monitored IP could have been anywhere in the apartment, so where the defendant's unlocked bedroom showed no indicia of separate ownership from the rest of the apartment, the search of his bedroom was proper. Id. at 396. With regard to the things to be searched, the SJC made the following finding: "Because that evidence, in the form of electronic files, could be easily transferred between devices at the same location, police need not have limited the devices to be searched. Id. at 396. The SJC raised the reasonableness of the search *sua sponte.* Id. at 397. It found that where "multiple electronic devices that may well belong to multiple individuals are seized and searched, the reasonableness of the undertaking will be judged, at least in part, by whether the searches of those devices are conducted in a manner that seeks to limit the scope of the search as much as practicable in the particular circumstances." Id. at 397–98. The SJC may in the future "consider whether to require, as some courts have, a digital search protocol that would affirmatively demonstrate 'a high regard for rights of privacy and take all measures reasonable to avoid unnecessary intrusion.'" Id. at 398 (quoting Commonwealth v. Vitello, 367 Mass. 224, 262 (1975)).

- Commonwealth v. Keown, 478 Mass. 232 (2017). "The scope of the search authorized by the warrant included files on the laptop related to the health or death of the victim; other prominent

poisoning cases; ethylene glycol or other poisons; and the financial records, life insurance plans, and wills of the victim and the defendant." Id. at 240. The affidavit "established probable cause to search for evidence on the laptop computer relating to the defendant's role in his wife's death." Id. "These categories of evidence were related to the means of committing the crime and the motive of the defendant, and provided sufficient guidance to the examiners so that they were not on a fishing expedition." Id. In addition, the search was conducted reasonably. Id. at 241. Examiners used a list of 50 search terms that was later supplemented by 19 additional terms. While not part of the warrant application, the terms were related to the categories of evidence sought in the affidavit. "[T]he examiner only looked closely at approximately 325 files of the nearly 400,000 found on the laptop computer." Id. The search in this case "took place more than a decade ago in an entirely different technological landscape"; thus, the absence of an ex ante search protocol did not defeat particularity. Id. at 41.

- Commonwealth v. Dorelas, 473 Mass. 496 (2016). The defendant, who was a suspect in an assault and battery by means of a dangerous weapon (firearm) and an assault with intent to murder, was involved in a shooting. Id. at 497. Interviews with his family and friends indicated that prior to the shooting he had received threatening calls and texts. Id. at 498. Police believed the defendant's iPhone contained evidence linking the defendant and the other shooter to the assaults and obtained a warrant authorizing a search for, among other things, saved and deleted photographs. Id. at 498–99. The search resulted in the discovery and seizure of incriminating photographs. Id. at 499. The defendant contended that police only had probable cause for his call logs and text messages, but not his photographs. Id. at 500. On direct appellate review, the SJC reached the following holding: "Communications can come in many forms including photographic, which the defendant freely admits. So long as such evidence may reasonably be found in the file containing the defendant's photographs, that file may be searched." Id. at 503. Therefore, such a search is "neither outside the scope of the warrant nor unreasonable." Id. The defendant further argued that a search using the Universal Forensic Extraction Device (UFED) could have been conducted for communications, including photographic communications, without reviewing his photograph file. Id. at 504. The SJC held that such a retrieval method was not constitutionally required where the photographic evidence would also reasonably be found in the phone's photograph file. Id. The Court was concerned that texts and their attachments might be overwritten over time and the evidence would thus only be found in the photograph file. Id.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the shooting. Id. at 764–65. They seized five computers and disks. Id. at 765. The defendant asserted that this was unlawful because the warrant did not specifically authorize the seizure of these items. Id. at 770. The warrant did authorize, however, seizure of several types of documents. Id. at 771. The Court held that the seizure of the computers was reasonable because they functioned as "closed containers" storing documents. Id. at 766, 771. [Note: In Preventative Medicine Assocs. v. Commonwealth, 465 Mass. 810 (2013), the SJC clarified that in McDermott, the fact that the warrant was issued before an indictment as part of an investigation and the Commonwealth's use of preset search terms during the preliminary review of the defendant's

files were important to its holding, id. at 830–32. The Court stated that it took "seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained." Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.]

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. 2001). Police received information that defendant was distributing child pornography over the Internet. Id. at *1. They obtained a warrant allowing them to seize the defendant's computers and associated storage devices, to bring those items to a search location, and to search them for "visual images depicting children in a state of nudity or sexual conduct." Id. at *8. The defendant challenged the warrant as not particular enough because it allowed for seizure and search of all files on the computer, many of which were not related to child pornography. Id. The court denied the defendant's motion, noting that "where the commingling of legitimate and illegitimate items makes an on-site examination impracticable, a temporary seizure of the whole is permitted." Id. (citing various federal cases to that effect). It noted that "[t]he investigators could not have known in what form—whether on the computer hard drive or other various storage devices—the defendant was storing the target images. To insulate such images from search and seizure merely because other, non-incriminating items may have sheltered the images would pervert the accepted purpose of the constitutional bar against general searches." Id. at *9.

- United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013). Police received a tip that a Washington resident was sharing child pornography over a peer-to-peer networking site. Id. at 1043. They prepared a search warrant affidavit setting forth the information they had received about the suspect's IP address, the pornography he shared, general peer-to-peer network operations, data storage, and known characteristics of child pornography offenders. See id. The magistrate granted the warrant, which authorized seizure of all of the defendant's computers and data storage devices, and police discovered large quantities of child pornography. Id. at 1043–44. The trial judge suppressed the evidence reasoning that the warrant was facially overbroad. Id. at 1045. The Ninth Circuit reversed this decision. Id. at 1046. It based this ruling on the "practical, common-sense decision" judges make in issuing warrants. Id. at 1046. Specifically, the Ninth Circuit found that "[t]he government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files" and reasoned that "[t]he government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner." Id. Given this reasoning and supportive precedent, the court found the warrant permissible. Id. at 1047.

- In re a Warrant for All Content & Other Info. Associated with Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386

(S.D.N.Y. 2014). Federal agents investigating illegal money remitting applied for a search warrant to access a suspect's entire email account in search of specified emails. Id. at 388. The Magistrate considered and rejected the reasoning that such a search was akin to a general warrant and therefore failed the Fourth Amendment's particularity requirement. Id. at 390–91. First, the judge noted that extensive authority supported the proposition that investigators could briefly examine a wide variety of documents during a search in order to determine relevance. Id. at 391–92. Though that examination is essentially a seizure, it is also a practical necessity to determine which documents can be more permanently seized. Id. at 392–93. Next, he noted that courts have been more flexible with searches and seizures of electronic evidence because the large mass of undifferentiated information makes an on-site search impossible. Id. at 392. Courts have recognized the practical necessity of copying hard drives for later examination, allowing the government to access electronic information outside the scope of its search in order to effectuate that search. Id. at 393. Finally, the judge found that email provider employees would not be capable of performing the search themselves because they would not know enough about the investigation in order to properly recognize relevant emails. Id. at 395.

(4) Staleness of Information Supporting Probable Cause

In order to provide probable cause sufficient for a search warrant, the information contained in an affidavit supporting such a warrant must be sufficiently fresh. See United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (detailed below). In assessing staleness, courts "do not measure the timeliness of information simply by counting the number of days that have elapsed" but rather "assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." Id. (citing United States v. Pierre, 484 F.3d 75, 83 (1st Cir. 2007)). This requirement should not be confused with the separate Massachusetts statutory requirement (examined next) that warrants be timely executed after they have been issued. The following cases address staleness in the digital evidence context.

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that affidavit in support of the warrant to search his home did not establish probable cause because it was based on stale information: namely, an image depicting child pornography that was uploaded from the defendant's computer to the Skype service seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time (id. at 29), the Court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the Court identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a

single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]" – an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020). Defendant was convicted of unlicensed carrying of a firearm outside his residence or place of business. Id. at 420–21.The police obtained a search warrant based an affidavit that described (1) a series of images and videos of the defendant and an acquaintance handling a TEC-9 firearm at the acquaintance's house, which the two of them posted on Snapchat, and (2) location data from a GPS device that the acquaintance, Santos, who was subject to GPS monitoring, was wearing at the time of the Snapchat posts. Id. The defendant argued that because "Snapchat videos and images that are posted on a particular date may have been taken, created, or recorded at an earlier date and uploaded much later… the Commonwealth failed to prove that the information officers relied on from the timestamps on the defendant's and Santos's Snapchat uploads was not stale." Id. at 424. The court rejected the defendant's arguments on staleness, finding probable cause was established by a Snapchat post by Santos from two days before the search warrant was obtained and executed: an image of a TEC-9 (semiautomatic) firearm captioned "Shyt change on my block trust issues I got put all my trust in semi autos." Id. at 421, 424. The court characterized the caption as "a present tense statement about Santos's perceived need for semiautomatic weaponry[, g]iven [which] there was probable cause to believe that the Snapchat image was taken contemporaneously with its posting" (which, in turn, was only two days before the warrant was executed). Id. at 424. The court did not discuss whether, or under what circumstances, similar posts absent such a present-tense caption could have sufficed to establish probable cause.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police waited ten days to apply for a search warrant on a seized phone. See id. at 283. This delay was permissible because "the defendant's minimal possessory interest was far outweighed by the government's interest in obtaining evidence regarding a recent murder." Id.

- United States v. Morales-Aldahondo, 524 F.3d 115 (1st Cir. 2008). Defendant was convicted of possessing child pornography as a result of an investigation targeting a child pornography website and its subscribers. Id. at 117–18. The download information obtained from the website was over three years old by the time the search warrant in this case was issued. Id. at 119. On appeal, the court upheld the trial judge's denial of the defendant's motion to suppress for staleness. Id. Focusing on the characteristics of child pornography collections, the court found that the warrant application (along with testimony by the same officer during a subsequent Franks hearing) "provided considerable support for the government's position that customers of child

pornography sites do not quickly dispose of" their collection. Id. Given this support, the court found that three years was not so long a period that the information had become stale. Id.

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished). In this case, the Attorney General's Office investigated the defendant based on a tip they had received from a New Hampshire police officer. Id. at *1. Using information from online exchanges the defendant had with the officer four months prior, the AG's Office obtained a search warrant for the defendant's premises where they located the evidence at issue in this case. Id. at *1, *6. The defendant alleged that the warrant was defective because, among other reasons, "there was no temporal proximity between the events constituting probable cause and the issuance of the warrant." Id. at *5. The court rejected this argument for two reasons. First, it found that the affidavit demonstrated continuous contact between the defendant and the undercover officer for several months. Id. at *6. Even though that information was itself four months old, the court found that it gave rise to an inference that the contact had continued. Id. Second, the court focused on the special circumstance of transmitting child pornography via computer. Id. at *7. Specifically, the affidavit described how computers retain data and how collectors of child pornography tended to retain those collections for long periods. Id. The court found that these descriptions "provided the magistrate with reason to conclude that the passage of time did not constitute a disabling tardiness." Id.

(5) Timely Execution of the Warrant

Mass. Gen. Laws ch. 276, § 3A, provides that "[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event not later than seven days from the date of issuance thereof . . . ." Mass. Gen. Laws ch. 276, § 3A (2018); see also Fed. R. Crim. P. 41(e)(2)(A) (requiring return of a warrant within fourteen days in federal courts). Given the complexities inherent in searching digital devices, the requirement that warrants be executed within seven days of issue could prove burdensome when investigating computer crimes. Fortunately, Massachusetts courts have interpreted the provision liberally with regard to digital evidence, as the cases below demonstrate.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. Relying on the reasoning in Commonwealth v. Kaupp, 453 Mass. 102 (2009), the court concluded that "if police have obtained a warrant to search and seize evidence from a cell phone in their custody, they must *attempt* but need not *complete* a forensic examination of the device within seven days of the warrant's issuance," id. at 330 (emphasis added) (Commonwealth v. Kaupp is summarized below). The court provided no guidance about what exactly constituted an "attempt" to conduct a forensic examination.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it. Id. at 105–06. Though the Supreme Judicial Court invalidated the warrant on probable cause grounds, it noted that, had the warrant been valid, the fact that it took more than seven days to fully search the computer would not have required suppression. Id. at 114–15. The Court cited other jurisdictions in support of the proposition "that the police do not need to complete forensic analysis of a seized computer and other electronic data storage devices within the prescribed period for executing a search warrant." Id. at 115. The Court held that a written return listing the devices to be examined that was filed within seven days after the search warrant issued satisfied Mass. Gen. Laws ch. 276, § 3A. Id.

(6) Manner of Executing the Warrant

"Under both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, the manner in which a search is conducted must be reasonable." Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). The cases below deal with this requirement in the digital evidence context.

- Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810 (2013). This case dealt with the search of a defendant's email account after indictment, and the possibility of intercepting privileged communications. Id. at 811. The Court held that "[w]hen an indicted defendant's e-mails are the object to be searched by the Commonwealth, because there is a risk that they contain privileged communications . . . a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege." Id. The SJC distinguished McDermott in part on the ground that the warrant in that case was issued before an indictment as part of an investigation, and the Commonwealth used preset search terms during the preliminary review of the defendant's files. Id. at 831. The Court stated that it took

  > seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained.

  Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the

shooting. Id. at 751, 764–65. As part of that search, they seized computers and disks. Id. at 765. The Court upheld this seizure as reasonable because it recognized the impracticality of searching computers on-site. Id. at 776. It also analogized this seizure to that of a firearm, stating that it "must be listed in the inventory taken from the premises in the timely return of the warrant but it may be submitted for specialized examination at an off-site forensic setting for the further extraction of evidence." Id. (citation omitted). The Court stressed the need to minimize the intrusion caused by digital searches. Id. at 777. In this case, police met that burden through the procedure they employed: "A forensic duplicate was made of the . . . hard drives and storage media to preserve all original data," and investigators used a keyword search that "resulted in a cursory inspection of only approximately 750 files . . . which amounted to less than one per cent of the defendant's files." Id. The Court also suggested that "[i]n conducting the actual search . . . considerable discretion must be afforded to the executing officers regarding how best to proceed" and that "[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary." Id. at 776.

b) Exceptions to the Warrant Requirement

"Warrantless searches are per se unreasonable unless they fall within one of the few narrowly-drawn exceptions to the warrant requirement." Commonwealth v. Durham, No. 9610398, 1998 WL 34064623, at *2 (Mass. Super. Ct. Oct. 13, 1998). "When a warrantless search is conducted, the Commonwealth has the burden of showing that the search, and any resulting seizure, falls within this narrow class of permissive exceptions." Id. The sections below examine searches incident to arrest, the plain view doctrine, and exigent circumstances in the digital evidence context.

(1) Search Incident to Arrest

One of the recognized exceptions to the warrant requirement is for searches made incident to a suspect's arrest. In Massachusetts, such searches are governed not only by the Fourth Amendment and art. 14 but also by Mass. Gen. Laws ch. 276, § 1, which is generally seen as more restrictive than the Fourth Amendment. See Commonwealth v. Blevines, 438 Mass. 604, 607 (2003). This statute permits searches incident to arrest "only (1) for the purpose of seizing evidence of the crime for which the arrest has been made in order to prevent its destruction or concealment or (2) for the purpose of removing any weapon the person arrested might use to resist arrest or to escape." Id. (quoting Commonwealth v. Wilson, 389 Mass. 115, 118 (1983) (internal quotation marks omitted)).

Whether the search is permissible is based on an objective standard, so an officer's subjective intent as to the search is irrelevant as long as the search could reasonably have been expected to uncover weapons or evidence facing destruction. Id. at 608 (permitting removal of defendant's car keys from his pocket during search because an officer "discovering a hard object in [a] defendant's rear pocket, [is] justified in retrieving that object as a potential weapon"). Further, having removed an item, "police need not ignore obvious aspects of or markings on" it, id. at 609 (citing Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 770 (1989)), but "detailed scrutiny" is disallowed, id. The cases below involve digital evidence in the context of a search incident to arrest.

- Riley v. California, 134 S. Ct. 2473 (2014). In two consolidated cases, law enforcement officials inspected the contents of an arrestee's cell phone—citing the search incident to arrest (SITA) exception—and used information therefrom in aid of further investigation. Id. at 2480–82. The Supreme Court held that these searches did not fall within the SITA exception because the justifications undergirding the exception did not apply to cell phones. Id. at 2484–85. First, digital contents of a cell phone cannot pose an immediate risk of physical injury to an officer. Id. at 2485–86. Second, once the phone has been seized by law enforcement (which the Court did allow), the arrestee cannot hide or destroy any evidence thereon (at least according to the Court). Id. at 2486. Confronting the issues of automatic locking, encryption, and remote wiping, the Court expressed doubt that these issues were particularly common, drew a distinction between such actions and the arrestee-initiated destruction of evidence in a typical SITA exception case, and allowed police to employ other means of preventing such actions. Id. at 2486–88 (noting that police may power off the phone or block its network connection and hypothesizing that the police may be allowed to alter a phone's settings to prevent it from locking). Finally, the Court noted that in exceptional cases—such as an imminent threat that the phone will be remotely wiped—the exigent circumstances exception may apply on a case-by-case basis. Id. at 2487–88.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone, James provided it, and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The

image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC held that the warrantless search of the digital camera was not a valid search incident to arrest under art. 14 of the state constitution. Id. at 592–93; see also id. (declining to address the constitutionality of the search under the Fourth Amendment). The SJC applied Chimel and Riley and found the twin threats of "harm to officers and destruction of evidence" were not present with regard to the data on a digital camera. Id. at 592. The SJC reasoned that, once the camera was secured, the data on it posed no danger and the risk of destruction of evidence was mitigated (and was less of a concern with respect to digital cameras lacking network connectivity than with cell phones). Id. at 592–93.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Police apprehended the defendant after giving chase to two men. Id. at 550. Defendant claimed he was not one of the two men. Id. When asked why he was breathing heavily, he claimed to have been arguing on the phone with his girlfriend. Id. at 550–51. After he was booked, the defendant placed a phone call he claimed was to his girlfriend. Id. at 551. Police then examined his cell phone call log about five hours after the arrest, without obtaining a warrant; the log belied both of defendant's statements. Id. The booking sergeant testified that it could take several days to get a warrant, and that he was concerned that incoming calls would "push out" previous calls on the call log, which he believed permitted only a limited number of calls. Id. The SJC held that under Riley (described above), decided a year earlier, the search of the call log was not a proper search incident to arrest and was not justified by exigent circumstances. Id. at 557. The SJC found that—absent testimony suggesting the phone was password protected or that police were concerned about remote wiping—preservation of the call log could have been achieved by "turning the cell phone off, placing the cell phone in a Faraday bag, or securing the cell phone and seeking a warrant for it." Id. at 558–59.

(2) The Plain View Doctrine

Under the plain view doctrine, law enforcement may make a warrantless seizure of evidence when four conditions are met. See Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 333 (2014) (explained below). First, the officers must lawfully be in a position to view the evidence. Id. Second, they must have a lawful right of access to the object. Id. Third, they must have a reason for seizing it. Id. In cases concerning (a) items possessed illegally, the incriminating character of the object should be immediately apparent. Id. (citing Horton v. California, 496 U.S. 128, 136 (1990) (explained below)). In cases concerning (b) other types of evidence, the particular evidence must plausibly be related to criminal activity of which the police are already aware. Id. (citing Commonwealth v. Sliech-Brodeur, 457 Mass. 300, 306–307 (2010)). Fourth, art. 14 requires that police come across the object inadvertently. Id. (citing Sliech-Brodeur, 457 Mass. at 307). The following cases address the plain view doctrine in the digital evidence context.

- Commonwealth v. Tarjick, 87 Mass. App. Ct. 374 (2015). Defendant's stepdaughter disclosed he abused her and took sexually explicit photos/made recordings of her. Id. at 375. Police obtained a warrant authorizing the search of the defendant's home and the seizure of the defendant's cell phone, the family computer, and the family video camera. Id. Three memory cards that were in the camcorders or digital cameras were also seized when the warrant was executed, though they

were not included in the warrant. Id. A second warrant was obtained to search the contents of the memory cards and evidence from the cards was later used at trial. Id. at 375–76. The Appeals Court held that the seizure was within the plain view exception. Id. at 378. The cards, though not included in the original warrant, were plausibly related to the crime. Id. "The officers were . . . aware that data may be freely transferred from one device to another through memory cards, and they could reasonably have concluded that the memory cards might have contained the alleged recordings." Id. The inadvertence requirement was also satisfied because there was "no indication that the police had probable cause to believe, prior to the search, that these specific memory cards or the cameras containing them would be found." Id.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. On appeal, the court upheld this seizure under the plain view doctrine. Id. at 333. Fulfilling the first and second plain view requirements, the warrant authorizing seizure of the tank top image means the police "were lawfully situated to view and to secure the [penis] images" because police are authorized to conduct cursory inspection of computer files to determine whether they match items listed in the warrant. Id. at 333–34 (citing Commonwealth v. McDermott, 448 Mass. 750, 776–77 (2007)). Third, the images of the defendant's penis were plausibly related to criminal activity of which the police were aware. Id. at 334. The defendant's statements of intent to exchange pictures of his nude body with pictures of the minor gave police reasonable ground to believe the pictures were evidence of enticing the minor to pose in a state of nudity. Id. The same statements made it plausible that the pictures were evidence of possession of matter harmful to minors with intent to disseminate. Id. Fourth, police discovered the images inadvertently because they "lacked probable cause to believe, prior to the search, that specific items would be discovered during the search." Id. (quoting Commonwealth v. Balicki, 436 Mass. 1, 9–10 (2002)).

- United States v. Burdulis, No. 10–40003–FDS, 2011 WL 1898941 (D. Mass. May 19, 2011). Defendant in this case emailed a police officer impersonating a young boy an explicit image. Id. at *1. Police obtained a warrant to search the defendant's computer. Id. at *2. During their search of image files on the computer, police uncovered child pornography. Id. After finding the seizure of those images authorized by the initial warrant, the court held in the alternative that the plain view doctrine also authorized the use of those images in evidence. Id. at *11–12. First, the officer searching the computer was lawfully in a position to view the evidence because he was conducting a search pursuant to a warrant. Id. at *11. As he was looking for image files, he was authorized to briefly examine all images to determine if they were a match. Id. Second, by this same logic, the officer had a lawful right of access to the files. Id. at *12. Third, the prohibited nature of child pornography images would have been immediately apparent. Id. [The court did

not examine the fourth requirement—inadvertence—because it exists only under Massachusetts law. See above for more detail on inadvertence.]

(3) Exigent Circumstances

"One well-recognized exception [to the warrant requirement] applies when 'the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" Kentucky v. King, 563 U.S. 452, 460 (2011) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)). Among the exigencies that the Court has identified in the context of searching a home are "emergency aid" (entering a home to render assistance to an injured occupant), "hot pursuit" (chasing after a fleeing suspect), and the need to prevent the "imminent destruction of evidence." Id.

- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020). Police seized defendant's phone, then answered an incoming call to the phone approximately one hour and fourteen minutes after the seizure. Id. at 437–48. The Commonwealth argued that exigent circumstances justified answering the call, but it did not offer "any evidence that it was impracticable to obtain a search warrant before the call was received." Id. at 441. The court allowed defendant's motion to suppress the call and evidence derived from it, explaining that "because there [was] no evidence in the record that obtaining a warrant was impracticable here, the Commonwealth failed to meet its burden of showing exigency, and [the court was] constrained to conclude that the motion to suppress should have been allowed." Id. at 442. The court noted, however, that the burden to show that it was impracticable to obtain a search warrant in one hour and fourteen minutes was not a heavy one and could potentially have been met by an officer's testimony about the steps necessary to obtain a warrant. Id. This case indicates that courts are unlikely to treat a "one hour or two hour time frame" as *by itself* sufficient to justify a search under exigent circumstances, id. at 439, but leaves open the possibility that the same search might have been found justified had the government produced evidence showing why that short timeframe made obtaining a warrant impracticable. Id. at 442 (but see Alvarez, 480 Mass. 1017 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer and absent any argument by the defendant that "observation of the outside of the… phone constituted a search")).

- Commonwealth v. Cruzado, 480 Mass. 275 (Aug. 10, 2018). Police found a cell phone lying near the defendant in a stairwell. Id. at 282. Having probable cause, the police seized the cell phone. Id. The Supreme Judicial Court held that "exigent circumstances supported the warrantless seizure: the risk of someone taking or tampering with the cell phone. Left unattended, especially in an area to which many people had access, the cell phone would have been at the risk of theft or vandalism." Id. at 283.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Possible degradation of a call log on a cell phone was deemed not an exigent circumstance because such degradation could be prevented in a number of different ways, such as by turning off the phone. Id. at 558–59.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's (a teacher) computers in a school classroom. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized both computers and subsequently obtained a search warrant. Id. at 105. The Court upheld the seizure of defendant's computer as appropriate because of exigent circumstances. Id. at 105–06. Specifically, the Court noted that "impoundment of an object pending the issuance of a search warrant violates the Fourth Amendment . . . only if it is unreasonable," which "turns on the facts of each case, requiring courts to 'balanc[e] the need to search or seize against the invasion that the search or seizure entails.'" Id. at 106 (quoting Commonwealth v. Catanzaro, 441 Mass. 46, 55–56 (2004)). The Court held that "[g]iven the ease with which computer files may be accessed and deleted, and the disruption that would have been created by posting an officer in the defendant's office and preventing students from entering pending the issuance of a search warrant . . . the seizure was reasonable." Id. In a footnote, the Court noted that while exigent circumstances justified the seizure, they would not have justified the subsequent search had it been warrantless because "[t]he exigency necessitating [the computer's] seizure dissipated once the computer had been secured." Id. n.7.

(4) Emergency Aid Exception

The emergency aid exception to the warrant and probable cause requirements originated in the context of searching a home, "permit[ting] the police to enter a home without a warrant when they have an objectively reasonable basis to believe that there may be someone inside who is injured or in imminent danger of physical harm." Commonwealth v. Peters, 453 Mass. 818, 819 (2009). The exception has since been extended to "uphold warrantless searches of places other than homes, in order to find and assist a victim of serious physical harm or to prevent such harm from occurring," and most recently to searches of the digital information. Commonwealth v. Raspberry, 93 Mass. App. Ct. 633, 639-40 (2018).

- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018). Police officers listening to a wiretap had "grave concerns about the defendant imminently causing serious bodily harm" to another with a firearm. Id. at 635 (internal quotation marks omitted). To locate the defendant and prevent the harm, police "asked AT&T to perform 'emergency pings' and give the police real-time CSLI about the approximate location of the defendant's cell phone." Id. The Commonwealth did not contest that a Fourth Amendment "search" took place, instead arguing that the "search" was "reasonable" under the emergency aid doctrine. See id. at 638, 640. The Massachusetts Appeals Court agreed. See id. at 641 ("We have no difficulty concluding that these standards were met here . . . What police did not know here, at the time of the call, was the whereabouts of the defendant. In the circumstances, it was objectively reasonable for the police to request real-time CSLI, in order to determine the defendant's current location and the direction in which she was moving, and thus to find and intercept her before she could shoot Dorsey.").

The emergency aid exception differs from the exigent circumstances exception: the former requires no probable cause to conduct a search, whereas the latter permits a warrantless search where probable cause exists but the circumstances make obtaining a warrant impracticable. Raspberry, 93 Mass. App. Ct. at 638, n. 8.

(5) Inventory Exception

Seizures of items on an arrestee's person may also be permissible, subject to police inventory policies. "[B]efore a person is placed in a cell, the police, without a warrant, but pursuant to standard written procedures, may inventory and retain in custody all items on the person . . . ." Commonwealth v. Seng, 436 Mass. 537, 550 (2002). For such seizure to be lawful, police must follow the rules of a written inventory policy that is "explicit enough to guard against the possibility that police officers would exercise discretion with respect to whether to open closed [containers] as part of their inventory search." Commonwealth v. Rostad, 410 Mass. 618, 622 (1991). "Inventory searches are intended to be noninvestigatory and are for the purpose of safeguarding the defendant's property, protecting the police against later claims of theft or lost property, and keeping weapons and contraband from the prison population." Barillas, 484 Mass. at 256. As such, "[i]n making an inventory — taking from the person, noting what is received, and placing it in safekeeping — the police are to act more or less mechanically, according to a set routine, for to allow then a range of discretion in going about a warrantless search would be to invite conduct which by design or otherwise would subvert constitutional requirements." Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 772 (1989) (cited in Barillas, 484 Mass. at 259).

Investigatory use of items seized under the inventory exception is impermissible unless the police have a search warrant or "obtain consent from the appropriate person (as determined by the inventory policy)." Barillas, 484 Mass. at 257. Any evidence resulting from investigatory use of inventory items without consent or a warrant is subject to suppression. Id.

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC rejected the argument that the search of the camera was a valid inventory search, holding that it was instead investigatory in nature because the camera was suspected stolen and the search was meant to identify the owner. Id. at 595–96.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found the defendant hiding in his home, conducted a pat frisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to

unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

(6) Consent

Warrantless searches are permissible with appropriate advance consent.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure was lawful under the search incident to arrest exception. Id. at 255.However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable

expectation of privacy in his movements. Id. at 77. The Court further held that the consent search of the defendant's residence was tainted by the illegal CSLI search. Id. at 71. Believing that the defendant and a second individual were transporting narcotics from Florida to Massachusetts, police obtained a court order pursuant to 18 U.S.C. § 2703 (2006) requiring the second individual's cellular service provider to "ping" the location of his cell phone. Id. at 73-74. After the two returned to Massachusetts, police knocked on the defendant's door and told him they knew he had just "purchased a large amount of narcotics" in Florida and was possibly storing it at his apartment. Id. at 74. The defendant then consented to a search, and police discovered a large amount of cash and two bricks of cocaine in his residence. Id. at 75. The SJC considered three factors in determining whether the defendant's consent was attenuated from the tainted CSLI data: "(1) the amount of time that elapsed between the defendant being confronted with the illegally obtained CSLI evidence and his grant of consent; (2) the presence of any intervening circumstances during that time period; and (3) the purpose and flagrancy of the official misconduct." Id. at 81-82 (internal quotes omitted). As to factors (1) and (2), the Court held that the lack of time and intervening events between the acquisition of the CSLI data and the police officer's confrontation with the defendant claiming that he had just returned from Florida with drugs weighed heavily against attenuation. Id. at 82-83. As to factor (3), while the Court "recognize[d] that the illegal police misconduct here was neither purposeful nor flagrant," it was still not dispositive in attenuating defendant's consent from the tainted CSLI data. Id. at 84. In her dissent, Justice Cypher explained that she would not reach the conclusion of the majority that a passenger in a tracked car has standing to challenge a CSLI search. Id. at 86 n.1 (Cypher, J., concurring in part and dissenting in part). In addition, she encouraged the SJC to adopt the good faith exception to the exclusionary rule in cases where the police acted under a "reasonable good faith belief that their conduct was lawful at the time." Id. at 92. While Justice Lowy agreed that Massachusetts should adopt a good faith exception, he did not believe the issue was properly raised by the Commonwealth in this case. Id. at 85-86 (Lowy, J., concurring).

3. The Exclusionary Rule

Generally, the exclusionary rule prohibits the introduction of evidence obtained as a result of a violations of the Fourth, Fifth and Sixth Amendments to the U.S. Constitution, and their counterparts under the Massachusetts Declaration of Rights. See Commonwealth v. Lora, 451 Mass. 425, 439 & n.26 (2008).

a) Good Faith / Substantial and Prejudicial

The Supreme Court has limited the application of the exclusionary rule in federal cases where officers acted in good faith, but Massachusetts does not recognize the good faith exception under art. 14. See Commonwealth v. Porter P., 456 Mass. 254, 273 (2010). Instead, it looks to "the foundational purpose of the rule—to deter unlawful police conduct . . . as a guiding principle" to determine whether evidence should be excluded. Commonwealth v. Maingrette, 86 Mass. App. Ct. 691, 697 (2014) (citing Commonwealth v. Wilkerson, 436 Mass. 137, 142 (2002)). Where:

> an arrest is wrongly made on the basis of mistaken information chargeable solely to the police, the burden is on the government to show . . . that the [government's] mistake was reasonable in the circumstances, and that the violation was minor or insubstantial and nonprejudicial and that exclusion of the evidence would not be likely to deter future police misconduct.

Id. (citations omitted).

b) Inevitable Discovery

> "Under the inevitable discovery doctrine, if the Commonwealth can demonstrate by a preponderance standard that discovery of the evidence by lawful means was certain as a practical matter, the evidence may be admissible as long as the officers did not act in bad faith to accelerate the discovery of evidence, and the particular constitutional violation is not so severe as to require suppression."

Commonwealth v. Fontaine, 84 Mass. App. Ct. 699, 709 (2014) (citation omitted). Though there are no Massachusetts cases applying this doctrine to a computer search, the First Circuit case below applying a slightly different federal test is instructive:

- United States v. Crespo-Rios, 645 F.3d 37 (1st Cir. 2011). In this case, the FBI searched the defendant's computer and external hard drive for evidence of chats between both him and an undercover agent and him and minors. Id. at 40–41. The search for these chats was conducted pursuant to a warrant that also listed, among other things, child pornography as something being sought. Id. at 40. During this search, agents found child pornography. Id. Following his indictment, the defendant moved to suppress the evidence, arguing that there was insufficient probable cause to support the overly-broad search warrant. Id. at 41. The First Circuit overturned the lower court by applying the inevitable discovery doctrine. Id. at 42-44. In searching the computer and hard drive for the chat evidence—for which there was undoubtedly probable cause—the court found that government agents would inevitably have discovered the child pornography because searching for computer files allows brief scanning of all possibly relevant files on the computer. Id. [This analysis is quite similar to that of the plain view doctrine, discussed elsewhere in this guide.]

B. Search of Electronic Service Providers

1. General Overview of Stored Communications Act

In 1986, Congress enacted the Stored Communications Act (SCA). See Pub. L. 99-508, 100 Stat. 1848, Title II. It provides limited privacy protections to the customers of "electronic communication service[s]" (ECS) and "remote computing services" (RCS). Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 383 (2014). ECS providers are email services like Gmail or Yahoo! along with certain elements of social media platforms, like a user's Facebook "wall." See generally Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 8–11 (2013).

RCS providers are harder to define and include any company that provides "computer storage or processing services by means of" the Internet to the public. Pub. L. 99-508, 100 Stat. 1848, § 2710. Cloud storage providers like Dropbox clearly fit this definition. Jeffrey Paul DeSousa, Self-Storage Units and Cloud Computing, 102 Geo. L.J. 247, 250 n.19 (2013). Courts have also found that YouTube belongs in this category. Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 11 (2013).

For a discussion of the argument that text messaging services are "remote computing services" under 18 U.S.C. § 2703(b) see Commonwealth v. Fulgiam, 477 Mass. 20, 31–33 (2017). The SJC held that the Commonwealth may not obtain the content of text messages without a warrant because text messaging is an "electronic communication service" subject to the requirements of § 2703(a). Id. at 32–33. The SJC also decided that a warrant supported by probable cause was also required for the content of text messages under art. 14. Id. at 33–34.

2. Search warrants served on out-of-state Internet service providers

Out-of-state corporations providing ECS or RCS to Massachusetts residents are subject to the jurisdiction of Massachusetts courts and must comply with search warrants issued by them. See Mass. Gen. Laws ch. 276, § 1B (2018); see also 18 U.S.C. § 2703 (2018) (outlining process by which state courts exercise jurisdiction over ECS and RCS providers).

C. Encryption and Self Incrimination

1. The Foregone Conclusion Doctrine

The Fifth Amendment to the United States Constitution states, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." This does not mean that a defendant cannot be compelled to produce some types of incriminating evidence, however, because only compelled *testimonial* communication that incriminates is barred. See Commonwealth v. Gelfgatt, 468 Mass. 512, 519 (2014) (citing Fisher v. United States, 425 U.S. 391, 408 (1976)). Written or oral communication created in response to government demand is plainly testimonial. See id. at 520. Compelled action that communicates something can also be testimonial in nature. Id.

"Whether an act of production is testimonial depends on whether the government compels the individual to disclose 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Gelfgatt, 468 Mass. at 520 (quoting United States v. Hubbell, 530 U.S. 27, 43 (2000)). For example, giving blood, producing a voice exemplar, or standing in a lineup are all nontestimonial because the suspect in question "is not required to disclose any knowledge he might have, or to speak his guilt." Id. at 521 (citations omitted). By contrast, complying with the government's demand could be testimonial "where [the act of production] is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence." Id. (citing Hubbell, 530 U.S. at 36 & n.19).

Even in cases where the act of producing evidence that the government seeks to compel is testimonial, however, that production loses its testimonial character if the information that would be

disclosed by the production is a "foregone conclusion." Id. at 522. The forgone conclusion exception obtains "where the facts conveyed already are known to the government, such that the individual 'adds little or nothing to the sum total of the Government's information.'" Id. (quoting Fisher, 425 U.S. at 411). In other words, "the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production." Commonwealth v. Jones, 481 Mass. 540, 547 (2019).

Several State and Federal courts have "applied the foregone conclusion exception in the context of compelled decryption," but neither the United States Supreme Court nor the Circuit Courts of Appeal have ruled on the government's burden of proof that applies to the "foregone conclusion" exception under the Fifth Amendment. Jones, 481 Mass. at 550. One federal district court "concluded that the appropriate standard of proof under the Fifth Amendment is clear and convincing evidence. Id. (citing United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018).

- In re a Grand Jury Investigation, 92 Mass. App. Ct. 531 (2017). During a grand jury investigation, a judge ordered petitioner to enter his personal identifying number (PIN) access code into his iPhone smartphone. Id. at 532. A warrant had previously issued for a search of the phone. Id. The Appeals Court held that production of the PIN was within the foregone conclusion exception to the Fifth Amendment. Id. at 534. To meet its burden under the doctrine, the prosecution had to demonstrate knowledge of the ownership and control of the cell phone and its contents, as well as "knowledge of the fact of [PIN code protection], and knowledge of the [existence of the PIN code]." Id. (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 524 (2014)). The prosecution was not required to show that it knew the specific content of the cell phone, but it did need to demonstrate knowledge of the existence and the location of the content. Id.

Article Twelve (art. 12) of the Massachusetts Declaration of Rights—analogous to the Fifth Amendment—provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself." Article Twelve provides greater protection than the Fifth Amendment in some contexts, but this broader protection "does not change the classification of evidence to which the privilege applies," so only "testimonial or communicative" evidence is protected from compelled disclosure. Commonwealth v. Gelfgatt, 468 Mass. 512, 525 (2014) (citations omitted). Massachusetts also recognizes the "foregone conclusion" exception to art. 12. Id. at 526.

For the exception to apply in the context of an order compelling decryption of an electronic device, Article Twelve requires that "the Commonwealth . . . prove beyond a reasonable doubt that the defendant knows the password." Commonwealth v. Jones, 481 Mass. 540, 552. But the Commonwealth does not need to "prove any facts with respect to the contents" of the device to be decrypted. In addition, "the entry of the password alone does not convey the fact of 'ownership' of the device or its contents." Id. at 547 n.8.

2. Encryption

In an affidavit the Commonwealth submitted in Gelfgatt, the director of the Massachusetts Attorney General's computer forensics laboratory explained that "encryption" is:

> the process by which 'readable' digital media, that is, digital media or data that can be viewed and accessed, is scrambled in such a way as to render that digital media or data 'unreadable' without decryption. Encryption can be performed both by hardware and by means of software tools.

Commonwealth v. Gelfgatt, 468 Mass. 512, 516 n.9 (2014). The director described "decryption" as:

> the process by which encrypted, scrambled data is rendered 'readable' again. In order to decrypt data, the person seeking decryption performs some action such as the entering of a password, scanning of a fingerprint or [insertion of] a USB Thumb drive with a pass code key on it. The encryption software then translates this action into a 'key,' essentially a string of numbers or characters. The encryption software then applies this key to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again.

Id. In Gelfgatt, the Commonwealth represented that the defendant's encryption software was virtually impossible to decrypt. Id. at 516–17. The Commonwealth represented that files thus encrypted could only be viewed if an authorized user entered a password. Id. at 517. But compelling the user to enter or disclose their password presents a possible violation of the Fifth Amendment and art. 12. The Gelfgatt court examined the interplay of these issues in Massachusetts:

- Commonwealth v. Gelfgatt, 468 Mass. 512 (2014). Defendant in this case was allegedly involved in a mortgage fraud scheme. Id. at 513. Law enforcement believed proof of that scheme would be found on the defendant's computers, and they obtained a search warrant, but encryption on the computers foiled their search. Id. at 516–17. When interviewed by police, the defendant admitted to owning multiple computers, stated that the police would be unable to access them because they were encrypted, and stated that he was able to decrypt the computers but refused to do so. Id. at 517. The lower court found that compelling him to do so would violate his Fifth Amendment and art. 12 rights against self-incrimination. Id. at 518–19. The SJC reversed and held that he could be compelled to enter his password in the circumstances presented by this case. Id. at 519–26.

  First, the Court stated that compelling a defendant to enter a decryption password, in the abstract, implicated the Fifth Amendment because the defendant would be implicitly "acknowledging that he has ownership and control of the computers and their contents," which could itself be relevant to the Commonwealth's case against him. Id. at 522. Next, the Court considered the "foregone conclusion" exception (explained above) and held that it applied because the defendant had already admitted to owning multiple computers, that their contents were encrypted, and that he was capable of decrypting them. Id. at 523-24. As a result, the facts that would have been communicated by compelling him to decrypt the computers were already known to the government,

making them a foregone conclusion. Id. Finally, the Court examined the issue under art. 12 but held that the same analysis applied. Id. at 524–26. [Note: Crucially, the Commonwealth proposed a protocol for decrypting the files that limited the scope of what was communicated through the compelled decryption. That protocol is outlined above.]

- Commonwealth v. Jones, 481 Mass. 540 (2019). Defendant was charged with trafficking a person for sexual servitude, Mass Gen. Laws ch. 265, § 50(a) (2018); id. at 541, and deriving support from the earnings of a prostitute, Mass. Gen. Laws ch. 272, § 7 (2018); id. at 541. The Commonwealth seized an LG cell phone from the defendant at his arrest and later obtained a warrant to search the phone. Id. at 541, 544. The LG phone had to be decrypted with the entry of a password before the search could be executed. Id. at 541. The Commonwealth moved for a Gelfgatt order, compelling the defendant to decrypt the LG phone under the "forgone conclusion" exception to the privilege against self-incrimination under the Fifth Amendment to the U.S. Constitution and Article 12 of the Massachusetts Declaration of Rights. Id. at 541–42. The SJC found that in order to obtain a Gelfgatt order compelling a defendant to decrypt an electronic device, the Commonwealth must "prove that the defendant knows the password beyond a reasonable doubt for the foregone conclusion exception to apply." Id. at 542–43. The Court also concluded that the Commonwealth met its burden in this case. Id. at 543. Finally, the SJC concluded that judges can consider new information in deciding renewed Gelfgatt motions, "without first finding that [the new information] was not reasonably available to the Commonwealth at the time the earlier Gelfgatt motion was filed." Id.

  To meet its burden of proving beyond a reasonable doubt that the defendant's knowledge of the password was a "foregone conclusion," the Commonwealth offered the following evidence: a witness testified to the defendant's regular use of the LG phone to answer calls and communicate through text messages (the record revealed several communications between the witness's phone and the LG phone related to prostitution); the defendant's phone number was listed with his name in the witness's contacts; the LG phone was in the defendant's possession at the time of arrest; the defendant had characterized the telephone number of the LG phone as his number to police when he was being booked following an arrest in an unrelated matter; police records showed that a backup number listed for the LG phone was registered to a person with the same name, social security number, and date of birth as the defendant; CSLI records revealed that the LG phone was in the same location at the same time as another phone that was found to be the defendant's phone. Id. at 556–57. All of this evidence, "taken together with the reasonable inferences drawn therefrom, prove[d] beyond a reasonable doubt that the defendant [knew] the password to the LG phone." Id. at 557 (noting that "it is hard to imagine more conclusive evidence" showing that the defendant knows the LG phone's password). The SJC also noted that even if the LG phone was used by more than one person, proof of ownership or exclusive control was not required. Id. at 547 n.8.

3. Sample Decryption Protocol

In Commonwealth v. Gelfgatt, the Commonwealth employed the following protocol to limit the amount of information that would be communicated by the compelled decryption:

> 1. The defendant, in the presence of his counsel, shall appear at the [Digital Evidence Laboratory] of Massachusetts Attorney General [Maura Healey] within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
>
> 2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
>
> 3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
>
> 4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
>
> 5. The defendant is expressly ordered not to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program;
>
> 6. The Commonwealth shall not view or record the password or key in any way; [and]
>
> 7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter.

Id. at 517 n.10.

D. Searches Implicating Attorney-Client Privilege

Searches that may intercept privileged communications between a suspect and his lawyer should be handled with special care. See generally Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 811 (2013). This problem is especially acute when a search is executed after a suspect has already been indicted and retained counsel. See, e.g., id. Even when a post-indictment search targets a different crime than the one for which the defendant was indicted, such a search runs a risk of encountering

privileged communications. Id. at 817–18. The section below detail how such a search should proceed in Massachusetts.

1. Post-Indictment Email and File Searches

The Commonwealth may seize emails of a defendant under indictment by means of an ex parte search warrant. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 821–22 (2013). Because of the sensitive nature of such a seizure, however, "only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment." Id. at 822. The affidavit supporting the warrant application must inform the judge at the outset that the subject of the email search is under indictment and must explain the connection, if any, between the indictment and the search warrant being sought. Id. Finally, the affidavit must explain why a search warrant rather than a rule 17(a)(2) summons is necessary to obtain the emails. Id. One possible explanation the SJC has suggested is cases where the Stored Communications Act requires a warrant, which it does for emails not yet opened that are 180 or less days old. See id. at 819 n.17 (citing 18 U.S.C. § 2703(a)), 822.

Once seized, emails possibly containing privileged material may be searched only after the Commonwealth receives a Superior Court judge's approval of a search protocol including specific procedures to protect against searches of privileged communications between a defendant and his attorneys. Id. at 823. One such procedure that the Court has approved is laid out below in the "Taint Team" section.

2. Taint Teams

A "taint team" is a group of attorneys or agents employed by a government office who have not at any time been involved in the investigation and/or prosecution of the defendants and who will not be assigned to any such investigation or prosecution in the future who sort the defendant's communications into privileged and unprivileged so that the latter group may be investigated by the government without eroding a defendant's attorney-client privilege. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 824–25 (2013).

There is "widespread skepticism" about the ability of government agents to properly review privileged communications without affecting that privilege, id. at 825, but the SJC has concluded that taint teams can "offer adequate protection to the Commonwealth's citizens," id. at 827. To that end, the SJC has put in place a two-tiered set of requirements surrounding the use of taint teams.

First, before a judge may authorize a team that will use members of a prosecutor's office as its members, "the Commonwealth must establish the necessity of doing so" because "use of an independent special master offers a far greater appearance of impartiality and protection against unwarranted disclosure and use of an indicted defendant's privileged communications." Id. at 829. In ruling on the prosecution's request to use a taint team, "the judge may consider factors such as the number of documents to be searched, the relative cost of a special magistrate, and the Commonwealth's unique ability to perform such a search due to specialized computer forensic examiners in its employ." Id. Further, the judge will consider "the Commonwealth's ability to erect an impenetrable wall between members of the taint team and members of the prosecution team." Id. at 829–30. In making this

determination, the judge will consider "the size of the particular prosecutor's office," and the Court expressed "less confidence that a small District Attorney's office can screen off members of the taint team as effectively as the Attorney General's office may be able to do." Id. at 830.

> Second, to pass constitutional muster, the taint team must comply with each of four requirements:
>
> (1) the members of the taint team must not have been and may not be involved in any way in the investigation or prosecution of the defendants subject to indictment—presently or in the future; (2) the taint team members are prohibited from (a) disclosing at any time to the investigation or prosecution team the search terms submitted by the defendants, and (b) disclosing to the investigation or prosecution team any e-mails or the information contained in any e-mails, subject to review until the taint team process is complete and in compliance with its terms; (3) the defendants must have an opportunity to review the results of the taint team's work and to contest any privilege determinations made by the taint team before a Superior Court judge, if necessary, prior to any e-mails being disclosed to the investigation or prosecution team; and (4) the members of the taint team must agree to the terms of the order in writing.

Id. at 828.

3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails)

"'Generally, disclosing attorney-client communications to a third party undermines the privilege.'" Dahl v. Bain Capital Partners, LLC, 714 F. Supp. 2d 225, 227 (D. Mass. 2010) (quoting Cavallaro v. United States, 284 F.3d 236, 246–47 (1st Cir. 2002)).

"'An exception to this general rule exists for third parties employed to assist a lawyer in rendering legal advice,'" including CC'ed emails. Id. at 227 (quoting Cavallaro, 284 F.3d at 247). In order for the exception to obtain, three criteria must apply: (1) the communication must be "necessary, or at least highly useful" for effective consultation between client and lawyer; (2) the exception only applies if the third party is playing an interpretive role between the lawyer and client (e.g., an accountant if he is helping the lawyer understand complex financial information); and (3) the communication must be made for the purpose of rendering legal advice, and not business advice or otherwise. Id. at 227–28.

II. Evidentiary Matters

A. Judicial Discretion

1. Trial Judge's Discretion

"A judge has broad discretion in the admission" of "demonstrative aids, including digital photographs and computer-generated images." Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing Commonwealth v. Noxon, 319 Mass. 495, 536 (1946)).

For an example of related flawed evidentiary practice, see Commonwealth v. Mienkowski, 91 Mass. App. Ct. 668 (2017). At a trial for aggravated rape of a child, posing a child in a state of nudity, and of dissemination of matter harmful to minors, the defendant's cell phone was admitted into evidence. Id. at 669. After some initial ambiguity about how the jury could examine the phone during deliberation, the judge adopted the Commonwealth's position and instructed the jury to limit their examination to the evidence already admitted (screenshots of relevant text messages). Id. at 675–77. On appeal, the defendant argued that the judge's initial admission of the cell phone without limitation and statements he made at the charge conference led defense counsel to rely in her closing on the jury's ability to examine the cell phone unconstrained and then "cut the legs out from under" her argument. Id. at 677–78. The SJC found it was possible that "neither the litigants nor the judge fully had considered the plethora of difficult issues that may be raised when a cell phone containing troves of unidentified electronic data is delivered into a jury's hands." Id. at 678. Though it held that it would have been preferable to resolve the ambiguity earlier, the SJC found no reversible error in the judge's handling of the issue. Id. at 678–69.

2. Demonstrative Photographs

"When, as here, the demonstrative photograph is generated as a digital image or video image, the judge must determine whether the image fairly and accurately presents what it purports to be, whether it is relevant, and whether its probative value outweighs any prejudice to the other party." Renzi v. Paredes, 452 Mass. 38, 52 (2008) (citing Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006)). "Concerns regarding the completeness or production of the image go to its weight and not its admissibility." Id. (citing Leneski, 66 Mass. App. Ct. at 295–96).

B. Discovery

1. Pornographic Images in Child Pornography Cases

"That forensic examination of the computer data by an expert retained by the defense is an essential component of effective assistance of counsel" in a child pornography case "is self-evident." Commonwealth. v. Ruddock, No. 08–1439, 2009 WL 3400927, at *3 (Mass. Super. Ct. Oct. 16, 2009). If an expert's access to evidence for purposes of examination is limited to the Commonwealth's facilities in order to prevent dissemination of such materials, the defendant's right to effective assistance of counsel will be unduly burdened. Id. A copy of the mirror image of a seized drive, including pornographic

images, must be given to the defendant's counsel of record and expert forensic examiner under a protective order limiting access to defense counsel and the expert. Id. (citing Mass. R. Crim. P. 14(a)(6)).

2. Wiretap transcripts

- Commonwealth v. Tavares, 482 Mass. 694 (2019). The defendant was convicted of murder in the first degree. During the investigation, police had recorded conversations between the defendant and a confidential informant using a wiretap. Id at 698. Prior to trial, the defendant moved successfully to suppress the recordings because "the investigation was not in connection in with organized crime" and thus violated G. L. c. 272, § 99. Id. at 714. After he was convicted, the defendant filed a motion for a new trial, arguing that his counsel was ineffective for failing to seek suppression of evidence derived from the recordings, as well as a "motion for postconviction discovery to obtain copies or transcripts of the wiretap recordings." Id at 714. The trial court denied both motions. Id. "Under the Massachusetts wiretap statute, a criminal defendant 'may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom' if the interception was made in violation of the statute." Id at 715 (quoting G. L. c. 272, § 99). On appeal, the SJC affirmed denial of the ineffectiveness motion, ruling that the defendant "failed to identify any specific evidence admitted at trial that was derived from the unlawful recordings." Id. But the Court reversed the denial of the motion for post-conviction discovery, concluding that the defendant is entitled to a copy of the wiretap transcript prior to any retrial. Id. at 715-716. The SJC found that the transcript would enable defense counsel to examine whether there is any improper reliance on the suppressed recordings at any future trial. Id.

3. Cell phone data

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.). The defendant, indicted on one count of rape, filed a Mass. R. Crim. P. 17(a)(2) motion to obtain information from the victim-witness's cell phone relating to her electronic communications and use of social media over a twelve-day period beginning with the day of the incident. Id. at *2–3. The motion judge ordered the victim-witness to produce her cell phone and/or any "backups" for forensic examination to recover the sought-after information. Id. at *3. The judge also ordered that the victim-witness provide the names and login information for third-party service providers that possessed the information, and directed Facebook to provide Facebook and Instagram data associated with the victim-witness's accounts, including photographs and the contents of messages. Id. The victim-witness, joined by the Commonwealth, petitioned a single justice of the Supreme Judicial Court for relief from the order under G.L. c. 211, § 3, asking that (1) the twelve-day period for which cell phone data was sought be more narrowly tailored to the time of the incident, and (2) the order be vacated insofar as it required the victim-witness to provide the names and login information for third-party service providers. Id. The single justice granted the requested relief. First, the justice summarized the Lampron requirements for a successful Rule 17 motion: relevance, admissibility, necessity, and specificity. Id. at *4. The justice then noted that Massachusetts case law had yet to address the use of Mass. R. Crim. P. 17 to obtain a victim-witness's cell phone communications or third-party service providers. Id. Observing that "individuals have significant privacy interests at stake in their cell phones," the justice concluded

that, "when ruling on a request under Rule 17 for a victim-witness's cell phone or cell phone records, the judge must include a consideration of these inherent privacy concerns." Id. The justice also examined decisions in which other state and federal courts had confronted similar issues, including a Minnesota Supreme Court decision holding that the fact that a "cell phone could contain exculpatory information was insufficient to order its production for examination." Id. at *5 (citing In re B.H., 946 N.W.2d 860, 870-71 (Minn. 2020)). Finally, the justice noted that Rule 17 "is a rule of production, not a rule of discovery." Id. After taking the above factors into account, and in light of the fact that the defendant could only speculate that relevant evidence might be obtained from the broad sweep of sought-after information, the justice granted the victim-witness's requested relief.

C. Authentication

1. Generally

To find that evidence is authentic, a judge must determine whether, by a preponderance of the evidence, there is sufficient evidence, including "confirming circumstances," to permit a "reasonable jury to conclude that this evidence is what the proponent claims it to be." Commonwealth v. Purdy, 459 Mass. 442, 449 (2011). Confirming circumstances are other facts that imply that evidence is what the proponent represents it to be. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011).

2. Photographs and Digital Images, Videos, and CDs

Authentication of photographs and videos is "typically… done through one of two means—having an eyewitness testify that the [photo or] video is a fair and accurate representation of what he saw on the day in question, or having someone testify about the [recording] procedures and the methods used to store and reproduce the [photo or] video material." Commonwealth v. Connolly, 91 Mass. App. Ct. 580, 586 (2017) (citing Commonwealth v. Pytou Heang, 458 Mass. 837, 855 (2011); Commonwealth v. Rogers, 459 Mass. 249, 267 (2011)). Digital photographs and videos are treated as equivalent to their analog counterparts. See Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294–95 (2006).

These are not the only possible ways to authenticate photo and video evidence, however. Commonwealth v. Davis, 97 Mass. App. Ct. 633, 635–36 (2020). More generally, admissibility may be established by any "evidence sufficient to support a finding that the matter in question is what its proponent claims." Mass G. Evid. § 901(a). For example, a witness may authenticate a digital photograph or video by testimony about the process used to create it and "showing that it produces an accurate result." Mass. G. Evid. § 901(b)(9).

- Commonwealth v. Davis, 97 Mass. App. Ct. 633 (2020): An officer at the scene of a crime saw a surveillance camera mounted on the outside of a nearby building, aimed at the street intersection where the crime had occurred. Id. at 635. He spoke with a resident of the building, viewed a video recording taken by the surveillance camera, and learned that the camera had been pointed at the intersection at the time of the crime. Id. Neither the resident nor the officer knew how to transfer the surveillance video recording to another medium, so Carty used his cellphone to record a video of the surveillance video recording; this cellphone video was played to the jury. Id. The following

was held sufficient to authenticate the cellphone video: the officer testified (1) that he had seen the scene that appeared in the video ("a car, with its driver's side door open, that had crashed into a pole at the intersection of Quincy Street and Baker Avenue"); (2) that the surveillance camera was aimed at the intersection in question, and (3) that still photographs also in evidence were fair and accurate representations of the scene of the shooting, where the still photographs depicted multiple vehicles and a sign that also appeared the video. Id. at 636.

- Commonwealth v. Leneski, 66 Mass. App. Ct. 291 (2006): A witness sufficiently authenticated a CD containing digital images created by a digital camera system at a convenience store where that witness testified he had "viewed the images on the computer and 'burned' the CD copy; [and] testified as to the procedure he used in the surveillance process, the copying process, and to the contents of the CD." Id. at 295.

Testimony about a photo or video that is not introduced in court, but instead is described to the jury by a witness, is subject to the admissibility conditions as the original photo or video: that is, the testimony is admissible upon establishing that the photo or video the witness saw was a fair and accurate representation of the events in question. Commonwealth v. Connolly, 91 Mass. App. Ct. at 586–87.

3. Digitally Enhanced Images and Video

The SJC has indicated that even digital photographs that have been enhanced have some use as a demonstrative aid, so long as they accurately illustrate what a witness testifies about. See Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing 2 McCormick, Evidence § 214 (6th ed. 2006)).

When offering digitally enhanced photographs or videos, the type of media and the manner of enhancement will be relevant. See Iacobucci v. Boulter, 193 F.3d 14, 20 (1st Cir. 1999). Objections to evidence on the grounds that it lacks a proper foundation are allowed at the discretion of the judge. Id. In Iacobucci, where the audio portion of a video was enhanced with a high quality play-back system to increase the volume, the trial judge decided that this did not destroy the video's integrity and the video was properly authenticated. Id. Several witnesses positively identified the defendants' voices on the recording, and the jury had the opportunity to evaluate the identification on their own. Id. at 20–21.

Alternatively, "[f]or digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007). In such a case, there will need to be proof that the digital enhancement process produces reliable and accurate results. Id.

4. Transcripts of Recordings

A written transcript of a recorded conversation taken from an electronic transmitting device can be authenticated where a witness testifies that the transcript is a fair and accurate representation of the recording. See United States v. Anderson, 452 F.3d 66, 76–77 (1st Cir. 2006) (citing United States v. Ademaj, 170 F.3d 58, 65 (1st Cir. 1999)). That witness does not have to be the person who transcribed the recording. Id. at 77.

5. Email

"While e-mails and other forms of electronic communication present their own opportunities for false claims of authorship, the basic principles of authentication are the same." Commonwealth v. Purdy, 459 Mass. 442, 450 (2011) (citing United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006)). Email authentication does not require expert testimony or evidence of exclusive access or password protection, although they are relevant to the jury's assessment of the weight of the evidence. See id. at 451. Where the relevance or admissibility of emails depends on whether the defendant authored the emails, the judge must "determine whether the evidence [is] sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the e-mails." Id. at 447 (citing Commonwealth v. Leonard, 428 Mass. 782, 785–86 (1999); Mass. G. Evid. § 104(b)(1)).

However, where the contents of an email do not sufficiently authenticate it, it may be properly authenticated through confirming circumstances. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011). Confirming circumstances imply that evidence is what the proponent represents it to be. Id. at 674. For example, the following confirming circumstances were sufficient to link a defendant to emails: (1) an email revealed that the sender would meet the email recipient at a certain place and time, and the defendant then appeared in that place at the time specified; (2) the sender of that email included his telephone number and a photograph of himself. Id. at 674–75. The defendant answered a call to that number, and emailed photograph depicted the defendant. Id.

Other confirming circumstances include: (1) emails originate from an account that bears the defendant's name and that the defendant admits having used; (2) emails are found on a computer hard drive that the defendant admits owning; (3) the defendant supplies all necessary passwords to access files on the computer; (4) emails contain an attached photograph of the defendant and/or describe the unusual circumstances or traits attributable to the defendant. Purdy, 459 Mass. 442, 450–51 (2011).

"Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking website such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant. There must be some confirming circumstances sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the emails." Id. at 450 (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)); see also Griffin v. State, 419 Md. 343, 357–58 (2011) (holding that authentication of a page printed from a social networking site requires more than a showing that a picture, birth date, and location of the alleged creator exist on the profile from which the page was retrieved).

Embedded e-mails will not be excluded because of the mere possibility that they can be altered without any specific evidence showing alteration. In Safavian, when "the trustworthiness of the emails particularly those . . . . emails that are included in a chain-either as ones that have been forwarded or to which another has replied" were challenged, the district court held that the "*possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course any more than it can be the rationale for excluding paper documents (and copies of those documents)."

435 F. Supp. 2d at 41 (emphasis in original). The court added that the defendant would be entitled, however, to raise any issue of alteration with the jury. Id.

6. Chatrooms

Similar to the method of authentication by confirming circumstances allowed in the Commonwealth, "[c]ourts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. For example, in [the Pennsylvania case] In re F.P., the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert . . . . The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 556 (D. Md. 2007) (citing In re F.P., 878 A.2d 91, 93–94 (Pa. Super. Ct. 2005)).

7. Text Messages

- Commonwealth v. Alden, 93 Mass. App. Ct. 438 (2018). The victim received threatening text messages from a "telephone number [she] had used to communicate with the defendant . . . every few days for over one year." Id. at 439. The trial court held that "the Commonwealth had established by a preponderance of the evidence that the text messages were authentic" - i.e., that the messages came from the defendant. Id. at 440. The Massachusetts Appeals Court affirmed because "for over one year, [the victim] had contacted the defendant multiple times each week using the telephone number from which the threatening messages originated. When she called that number, the defendant answered. When she sent a text message to that number to arrange a meeting with the defendant, he appeared." Id. at 440–41. Moreover:

  > [t]he content of the text messages reinforced their link to the defendant. It is undisputed that at the time she received the text messages, [the victim] was a witness in a pending case against the defendant. In this context, where there was evidence that the text messages directed her to "keep her [explicative] mouth shut" and "leave their personal stuff out of the courtroom" or "people [would] come after [her] if [she] went to court," it was reasonable to infer that the defendant was responsible for sending the messages.

  Id. at 441.

8. Information Available on Websites and Social Networks

Evidence available on websites presents its own problems. "Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007). "The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting." Id. (citing United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000)). In doing so, federal courts require the proponent of such evidence to show what was actually on the website, to show that the

exhibit or testimony accurately reflects that content, and to show that the content can be attributed to the owner of the site. Id. (citations omitted).

In the courts of the Commonwealth, "[e]vidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant." Commonwealth v. Purdy, 459 Mass 442, 450 (2011) (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)).

Circumstantial evidence can authenticate a social network page:

- Commonwealth v. Meola, 95 Mass. App. Ct. 303, No. 18-P-83, 2019 WL 2202909 (Mass. App. Ct. May 22, 2019). The Appeals Court affirmed the Superior Court's holding that sufficient evidence in the form of "confirming circumstances" established that the defendant attached an obscene video to a communication he sent to an underage victim. Following a jury waived trial, a Superior Court judge found the defendant guilty of disseminating obscene material to a minor in violation of G.L. c. 272, § 28. Id. at *1. The Appeals Court looked to the principles established by the SJC in Commonwealth v. Purdy, 459 Mass 442 (2011) regarding authenticating digital evidence (that is not self-authenticating). First, Purdy establishes that direct evidence is not necessary to determine that a defendant sent a digital communication. Rather, a judge "may consider circumstantial evidence and look to 'confirming circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored" the electronic communication. Meola, 2019 WL 2202909 at *5 (quoting Purdy, 459 Mass. at 450). Second, under Purdy, the "mere possibility that a digital communication was fraudulently sent by someone other than the person associated with a particular social media...account from which the communication originated is not a bar to its authentication." Meola, 2019 WL 2202909 at *5. Third, common-law principles concerning authenticity are applicable to digital communications. Id. In this matter, the trial judge's decision to exclude records proffered by the prosecutor, describing user information related to the Facebook account and the sender of the video, required the Commonwealth to rely on indirect evidence to authenticate the materials. Id. at *2. The Appeals Court concluded that the following facts offered sufficient indirect evidence of authenticity: the defendant's prior association with the victim (defendant had previously lived with her and her mother); the defendant's biological relation to the victim's half-sister; and the friend request the user of the account sent to the victim. Moreover, the Court determined that the trial judge did not err in finding the communications authentic because there was no evidence to suggest that the Facebook profile photo or the self-authored obscene video were publicly available. Id. at *6. Based on these facts, the Court affirmed the trial judge's determination that the defendant "purposefully disseminated matter harmful to a minor to the victim" with full knowledge that she was a minor. Id. at *7.

- Other jurisdictions have taken a similar approach. For example, in the Texas case Tienda v. State, MySpace webpages were admissible because there was sufficient evidence on them indicating that they "were what they purported to be." 358 S.W.3d 633, 646 (Tex. Crim. App. 2012). The court stated that, "as with the authentication of any kind of proffered evidence, the

best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case." Id. at 639. The court held that there was "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the Myspace pages belonged to the appellant and that he created and maintained them." Id. at 645; see also Parker v. State, 85 A.3d 682 (Del. 2014) (holding that social media post was sufficiently authenticated by circumstantial evidence and by testimony explaining how the post was obtained); Simmons v. Commonwealth, No. 2012–SC–000064–MR, 2013 WL 674721 (Ky. Feb. 21, 2013) (holding that the print-outs of the defendant's Facebook messages were admissible because the messages were what they purported to be and the role of the judge, as a gatekeeper, was only to determine if an offering party has produced enough evidence for a reasonable jury to find authenticity).

9. Software Programs Used in Investigation

When a witness uses software to create information relevant to an investigation, that witness should testify in detail as to the nature of the tool, how the witness used it, and how it was created and maintained in order to authenticate the records. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 327 (2009) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)). In Whitlock, a police officer used a software program called ArcView, which is a computerized map that depicted the location and ownership of property within the city of Springfield. Id. at 325–26. The information provided by this software was used to show that the defendant was distributing a controlled substance within a school zone. Id. Where software provides information to a witness, for example software that measures and provides distances between real-world objects, it does not make a "statement," and therefore is not subject to the hearsay rule. Id. at 326–27.

10. GPS and Probation

The SJC has held GPS technology to be "widely used and acknowledged as a reliable relator of time and location data" under the Daubert-Lanigan standard for admission of scientific testimony. Commonwealth v. Thissell, 457 Mass. 191, 198 (2010); see also Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592-3 (1993); Commonwealth v. Lanigan, 419 Mass. 15, 26 (1994). Judges may at their discretion admit testimony that "GPS data placed the defendant in particular locations at particular times" based on data from any GPS device whose positioning method has been demonstrated to be "no more than the application of existing and scientifically-accepted GPS monitoring technology -- a technology that has been accepted as reliable." Davis, 97 Mass. App. Ct. at 640. The fact, acknowledged by an appellate court, that GPS information is "subject to variations in accuracy depending upon atmospheric conditions, intervening obstacles, or reflection of the satellite signals from buildings, windows, or cars, [goes] to the weight of the evidence, not to the fundamental reliability of the GPS technology." Id. (citing Sacco v. Roupenian, 409 Mass. 25, 30 (1980); Rothkopf v. Williams, 55 Mass. App. Ct. 294, 299 (2002)). An appellate court has distinguished and left unresolved the issue of whether GPS records are also reliable indicators of speed (as opposed to location). Id. at 641.

Probationers' GPS records have been used as evidence of a defendant's location at particular times; evidence that can be relied on to show that the defendant violated conditions of probation or was at

the scene of a crime. Thissell, 457 Mass. at 198–99; Davis, 97 Mass. App. Ct. at 639–40. Official GPS records maintained by the Commonwealth and certified by an officer having legal custody of the record may minimize concerns about authenticity, Thissell, 457 Mass. at 199 ("recommend[ing] strongly that copies of GPS records offered in future revocation proceedings be properly attested and certified by an appropriate custodial officer"), but GPS-based information may also be authenticated on other ways. Davis, 97 Mass. App. Ct. at 637 (authenticating GPS data by the testimony of a GPS device manufacturer's manager of product development).

D. Technological evidence as the basis of criminal conviction

Evidence used as the basis of a conviction must be sufficient, viewed in the light most favorable to the government, for a rational trier of fact to find the essential elements of the crime beyond a reasonable doubt. Commonwealth v. Ayala, 481 Mass. 46, 51 (2018) (citing Commonwealth v. Latimore, 378 Mass. 671, 677-78 (1979). Thus, even evidence that meets the preponderance standard required to authenticate a piece of evidence, see § II.C, supra, may not be sufficient to support a conviction. The government bears the burden of explicit proof even for facts about technology that may be well known to the trier of fact, e.g., that a password is generally required to log in to and send messages from an Instagram account. Commonwealth v. McMann, 97 Mass. App. Ct. 558, 561 (2020). Such facts are not appropriate subjects of judicial notice. Id. at 561 n.4.

- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020). Defendant was convicted of violating an abuse prevention order that prohibited him from contacting his ex-girlfriend. Id. While the order was in effect, the ex-girlfriend received an Instagram message from user "bigm617" that said "Yoooo." Id. at 559. She testified that she knew that "bigm617" was the defendant's account "because the associated account displayed pictures of the defendant, including one of him with the victim, and the victim and the defendant had previously 'liked' and commented on each other's Instagram posts." Id. The victim showed this Instagram message to a police officer, who met with the defendant later that day. Id. The defendant denied sending any message to the victim, 'wanted to show [the officer] that he never did[,]' and entered a passcode to unlock his cell phone. He then opened the Instagram application on his cell phone, and the 'Yoooo' message to the victim appeared on the screen. The officer observed that the defendant looked '[s]urprised.' Id. The appeals court held that "even assuming without deciding that the Instagram message was properly authenticated, the Commonwealth failed to… prov[e] beyond a reasonable doubt that the defendant was the person who wrote or sent the message to the victim. Although the evidence was sufficient to show that the Instagram account was the defendant's and that he could access it, there was no circumstantial evidence establishing authorship." Id. at 560. The court suggested the burden could have been met by "evidence that the message itself contained characteristics showing that the defendant wrote it, or through evidence establishing how secure Instagram accounts are and how the Instagram cell phone application works." Id. at 562.

E. Best Evidence Rule

1. Best Evidence Rule - Generally

"The best evidence rule provides that, where the contents of a document are to be proved, the party must either produce the original or show a sufficient excuse for its nonproduction." Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001); see also Mass. G. Evid. § 1002. However, what constitutes a "document" has been narrowly construed such that "[t]he best evidence rule is applicable only to those situations where the contents of a *writing* are sought to be proved." Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970) (emphasis added). Most photographs and videos depict objects rather than writings. Consequently, the best evidence rule does not typically apply, *inter alia*, to photographs or videotapes. See also Commonwealth v. Weichell, 390 Mass. 62, 77 (1983) (holding that the "enlarged photograph was a fair and accurate representation of the defendant at the time of his arrest"); Commonwealth v Leneski, 66 Mass. App. Ct. 291, 294 (2006) ("Videotapes, like photographs, are not subject to the best evidence rule."). Additionally, "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes." Leneski, 66 Mass. App. Ct. at 294.

2. Digital Images

Digital image evidence is not subject to the best evidence rule in Massachusetts because these images are not writings. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006) (citing Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970)). The Leneski court held that digital images from a computer copied to a compact disk ("CD") would be considered as originals. Id. Testimony about authenticity, including how the disc was generated, the procedure used in the surveillance process, the copying process, and the contents of the CD, was deemed sufficient. Id. The Court noted that there was opportunity for cross-examination that went to the weight of the evidence on the subject of surveillance procedure and the method of storing and reproducing the data. Id.

This exception to the best evidence rule extends to images that have been transferred from a hard drive to other media such as CDs and DVDs. See id. at 294 (holding that "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes").

3. Admission of Duplicate Evidence

> [W]here the original [of a document] has been lost, destroyed, or otherwise made unavailable, its production may be excused and other evidence of its contents will be admissible, provided that certain findings are made.
>
> As a threshold matter, the proponent must offer evidence sufficient to warrant a finding that the original once existed. . . . If the evidence warrants such a finding, the judge must assume its existence, and then determine if the original had become unavailable, otherwise than through the serious fault of the proponent . . . and that reasonable search

had been made for it. . . . If the judge makes these findings in favor of the proponent, the judge must allow secondary evidence to establish the contents of the lost writing.

Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001) (quoting Fauci v. Mulready, 337 Mass. 532, 540–43 (1958) (internal citations and quotation marks omitted)).

4. Videos

The best evidence rule does not apply to digital videos. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006). "Our courts have held that videos are 'on balance, a reliable evidentiary resource . . . .'" Id. (quoting Commonwealth v. Harvey, 397 Mass. 351, 359 (1986)). "[Videos] 'should be admissible as evidence if they are relevant, they provide a fair representation of that which they purport to depict, and they are not otherwise barred by an exclusionary rule.'" Id. (quoting Commonwealth v. Mahoney, 400 Mass. 524, 527 (1987)).

5. Email

It is unlikely that printed email communications are subject to the best evidence rule so long as their authenticity can be proven through circumstantial evidence. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 675–76 (2011). In Amaral, the court reasoned that the email server, or the computer itself, is not better evidence than directly printed emails, and that "[t]he significance of the best evidence rule has declined appreciably in recent decades." Id. at 675 (internal quotation marks omitted).

6. Summaries

Large volumes of digital evidence may be summarized and shown to a jury without running afoul of the best evidence rule.

In the Commonwealth, voluminous evidence that would be difficult for a jury to understand due to volume or complexity may be presented in the form of a written or testimonial summary or a chart, shown by testimony to accurately reflect the contents of the underlying documents, so long as the proponent does not unfairly emphasize portions of the summarized evidence. See Mass. G. Evid. § 1006; Commonwealth v. Mimless, 53 Mass. App. Ct. 534, 538 (2002) (quoting Welch v. Keene Corp. 31 Mass. App. Ct. 157, 165–66 (1991)) ("[C]are must be taken to insure that summaries accurately reflect the contents of the underlying documents and do not function as pedagogical devices that unfairly emphasize part of the proponent's proof.") (internal quotation marks omitted); Commonwealth v. Greenberg, 339 Mass. 557, 582 (1959) ("The witness was not allowed to state deductions and inferences of his own but could state only the results of his computations from the admitted evidence."). The summarized evidence should be made available to other parties in advance of trial, and the court may order that the originals be produced in court. See Mass. Guide to Evid. § 1006.

- Commonwealth v. Suarez, 95 Mass. App. Ct. 562 (2019). The defendant, who was convicted of assault with intent to rape and other charges, challenged on appeal the introduction at trial of a six-minute compilation of video surveillance footage from before, during and after the attack, and a timeline describing parts of the videos. Id. at 566-67, 570. Since the defendant did not object at

trial, the Appeals Court "examine[d] whether any abuse of discretion in admitting the exhibits created a substantial risk of a miscarriage of justice." Id. at 570-71. The Court found the individual underlying videos could not 'be conveniently examined in court.'" Id. at 571 (quoting Mass. G. Evid. § 1006). Though the Commonwealth played portions of the videos in the courtroom, "a deliberating jury would have found it difficult to master the technology necessary to find and view the relevant parts of the videos in the jury room." Id. at 571-72. Furthermore, the Court rejected the defendant's claim that the compilation was unfairly edited. Id. at 572. However, the Court did find certain improprieties in the compilation and timeline. In particular, it ruled that still photos, taken from a 7-Eleven store four hours after the attack, should not have been included in the compilation because the photos taken hours after the assault were not relevant to the crime itself. Id. The Court also ruled that the timeline describing the digital compilation "could and should have used a neutral heading" for a set of video clips. Id. at 574. The Court criticized the Commonwealth's use of the term "suspect" in the timeline to refer both to a person the defendant admitted was him, in certain video clips, and to the attacker, in other video clips, since use of that term suggested that they were the same person. Id at 573. The Court ruled, however, that these "limited errors in the compilation and the timeline" did not create a substantial risk of a miscarriage of justice because they had little, if any, impact on the case. Id. at 574.

F. Hearsay

When software merely provides information to a witness, the software does not make a "statement," and therefore is not subject to the hearsay rule. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326–27 (2009) (holding that information provided by measuring software that indicated to the witness the distance between real-world objects were not statements subject to the hearsay rule) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)); see also Thissell, 457 Mass. at 197 n.13 (discussing the difference between computer-generated and computer-stored records in the context of the rule against hearsay); Commonwealth v. Royal, 89 Mass. App. Ct. 168, 171–72 (2016) (treating "computer-stored" records as hearsay, but treating "computer-generated" records as not hearsay); Commonwealth v. Woollam, 478 Mass. 493, 498 (2017) (holding that call logs are computer-generated records that do not raise hearsay concerns; admissibility thus only depends on authentication); Davis, 97 Mass. App. Ct. at 641–43 (holding that GPS logs and maps of the defendant probationer's location over time, which were created by a mapping company that added dots and the defendant's name to maps based on GPS location data, were not hearsay).

G. Business Records Exception

1. Email

A document from an email service provider that indicates that a specific login name is connected to a defendant's email address is admissible as a business record as long as it is supported by an affidavit from the service provider's custodian of records. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 673–74 (2011).

2. Computer Records

"[C]omputer records . . . are admissible under the business records exception to the hearsay rule, [Mass. Gen. Laws ch.] 233, § 78, if they were (1) made in good faith; (2) made in the regular course of business; (3) made before the action began; and (4) [it was] the regular course of business to make the record at or about the time of the transaction or occurrences recorded." McLaughlin v. CGU Ins. Co., 445 Mass. 815, 819 (2006) (quoting Beal Bank, SSB v. Eurich, 444 Mass. 813, 815 (2005) (internal quotation marks omitted)).

A lack of personal knowledge on behalf of the affiant, the maker, or custodian of records goes to the weight and not the admissibility of the business records. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674 (2011) ("[T]he personal knowledge of the entrant or maker affects only the weight of the record, not its admissibility.") (quoting and citing Note to Mass. Guide to Evid. § 803); see also McLaughlin, 445 Mass. at 819 (2006) ("[P]ersonal knowledge of the entrant or maker of a record is a matter affecting the weight rather than the admissibility of the record.").

A print-out of an electronic document is admissible as a business record as long as it is supported by an affidavit from the provider's custodian of record establishing that the requirements of the business records exception are met. Amaral, 78 Mass. App. Ct. at 673–74 n.4; McLaughlin, 445 Mass. at 8199 ("The affidavits plainly establish that the records satisfy these foundational requirements.").

H. Confrontation Clause

1. Software-generated information

"The confrontation clause bars the admission of testimonial out-of-court statements by a declarant who does not appear at trial unless the declarant is unavailable to testify and the defendant had an earlier opportunity to cross-examine him." Commonwealth v. Wilson, 94 Mass. App. Ct. 416, 417 n.1 (2018), (quoting Commonwealth v. Simon, 456 Mass. 280, 296 (2010).

When introducing software-generated information that is not hearsay as evidence, see § II.E, supra, the Confrontation Clause is not implicated. See Commonwealth v. Hurley, 455 Mass. 53, 65 n. 12 (2009) ("admission of a testimonial statement without an adequate prior opportunity to cross-examine the declarant… violates the confrontation clause only if the statement is hearsay…") (citing Crawford v. Washington, 541 U.S. 36, 59-60 & n. 9 (2004).

It is unclear whether the introduction of software-generated information that *is* hearsay (if that is possible at all) would implicate the Confrontation Clause. An appellate court has considered the question in dicta, and suggested that (1) software-generated information may not come from a "declarant" within the meaning of the Confrontation Clause at all, but (2) if a company involved in producing the information were treated as a declarant, then the requirements of the Confrontation Clause could be satisfied by having a representative of the company as a witness. Davis, 97 Mass. App. Ct. at 644.

2. Secondary Examiners

The Sixth Amendment's bar on the testimonial statements of a witness who does not appear at trial applies to forensic examiners because their explanation of the process and results of specific forensic examinations are testimonial statements. See United States v. Soto, 720 F.3d 51, 58–60 (1st Cir. 2013) (summarizing relevant Supreme Court cases).

A "surrogate" witness who is familiar with a lab's practices, but who has formed no independent opinion of the results is insufficient to satisfy the Sixth Amendment. Id. at 58 (citing Bullcoming v. New Mexico, 564 U.S. 647, 662–63 (2011)).

However, "[t]he government may ask an agent to replicate a forensic examination if the agent who did the initial examination is unable to testify at trial, so long as the [testifying] agent . . . conducts an independent examination and testifies [as] to his own results." Id. at 59; see, e.g., Commonwealth v. Chappell, 473 Mass. 191, 199–200 (2015) (substitute DNA expert testimony allowed because, as the second reader, she independently read all the raw data and the reports produced by the original analyst, made interpretations, and ensured that there was agreement between her findings and those the analyst, and therefore testified to her opinions or conclusions concerning the DNA).

- Commonwealth v. Seino, 479 Mass. 463 (2018). Defendant was convicted of first-degree murder. Id. at 464. On appeal, he asserted several confrontation claims. Id. at 466, 469–72. First, the defendant argued that it was improper for a doctor who did not perform the autopsy to refer during his trial testimony to statements in the autopsy report and death certificate, neither of which the testifying doctor authored. Id. at 466. The SJC held that it was appropriate for the testifying doctor to offer his opinion on the cause of death based on the case file and his own examination, but agreed with the defendant that the doctor should not have testified about statements in the autopsy report and death certificate. Id. at 466–67. The SJC found that the error was harmless beyond a reasonable doubt, however, because the improper testimony was cumulative, did not incriminate the defendant, and "did not contribute to the guilty verdicts." Id. at 467–68. Second, the defendant argued that his confrontation right was violated when two experts, as part of their trial testimony, used charts showing DNA testing data obtained by other analysts (who did not testify). Id. at 469–70. The SJC held that the data should not have been shown to the jury. Id. at 470. The Court also concluded, however, that there was no substantial likelihood of a miscarriage of justice "because the charts did not taint the analysts' independent opinions, which . . . were properly admitted." Id. at 471. [Note: The Court applied a miscarriage of justice standard because the defendant did not preserve an objection to the charts at trial. Id. at 470.] The SJC noted that the charts "merely displayed genetic locations, not any information regarding a match or the statistical probability thereof." Id. at 471. Third, the defendant argued that it was reversible error for an analyst to testify that the defendant's DNA profile matched a DNA profile developed by a different analyst from the victim's jeans. Id. The SJC rejected this claim, finding that the defendant had had the opportunity at trial to cross-examine the analyst who developed the defendant's DNA profile, the supervisor of the laboratory that developed the DNA profile from the jeans, and the analyst who compared the two profiles. Id. at 471–72.

- Commonwealth v. Scesny, 472 Mass. 185 (2015). An autopsy report and photographs from the victim's autopsy were introduced in evidence and a substitute medical examiner testified regarding findings in the report. Id. at 196–97. The SJC held the autopsy report was "'inadmissible hearsay whose admission violate[s] the defendant's right of confrontation under the Sixth Amendment to the United States Constitution,'" id. at 197 (quoting Commonwealth v. Emeny, 463 Mass. 138, 145 (2012)), and that a substitute medical examiner cannot testify about the facts and findings of the report on direct examination. Id. The autopsy photographs were properly admitted through a State police trooper who attended the autopsy. Id. at 198 n.25.

- Commonwealth v. Jones, 472 Mass. 707 (2015). At defendant's trial for rape, a chemist at the State police crime laboratory, who was not present during the "rape kit" examination and had no apparent connection to the hospital at which the swabs were taken, was allowed to testify on direct examination to her "understanding" of how the swabs had been collected. Id. at 711–12. The SJC held that allowing an expert witness who had not been present during the examination and had no apparent connection to the hospital where the examination occurred, to testify on direct examination to her "understanding" of how the swabs had been collected violated the defendant's confrontation right. Id. at 708. The SJC found that the "surrogate" expert's statements were testimonial for two main reasons: (a) in labeling the various swabs and completing the "rape kit" inventory list, the initial examiner made factual statements concerning how the swabs were collected, and (b) the purpose of a "rape kit" is to gather forensic evidence for use in a criminal prosecution,. Id. at 714. These statements would therefore only be admissible if they complied with the test established by Commonwealth v. Greineder, 464 Mass. 580, 593 (2013). Id. at 715. The Jones Court summarized the holding of Greineder as follows: "'[e]xpert opinion testimony, even if based on facts and data not in evidence, does not violate the right of confrontation, provided that the facts and data 'are independently admissible and are a permissible basis for an expert to consider in formulating an opinion,' and that two further conditions are met. First, the expert must 'not present on direct examination the specific information on which he or she relied'; second, the expert witness must have the capacity to 'be meaningfully cross-examined about the reliability of the underlying data.'" Id. at 713 (quoting Greineder, 464 Mass. 580) (other citations omitted). The statements in Jones did not meet either of these requirements in Greinder: (1) the underlying hearsay facts of how the swabs were collected came in on direct examination and (2) the expert could not meaningfully be cross-examined about the reliability of the representations of the "rape kit" examiner concerning the origins of the swabs and lacked the capacity to address chain of custody and evidence-handling protocols relevant to the process by which the swabs were collected. Id. at 715–16. The testimony thus failed to comply with Greineder and was therefore inadmissible. Id. at 715.

III. Cybercrimes

A. Possession of Child Pornography

1. Multiple Convictions Require Multiple "Caches"

In prosecuting possession of child pornography, each "cache" of pornography counts as one unit of prosecution. See Commonwealth v. Rollins, 470 Mass. 66, 73–75. That is, "a defendant's possession of a single cache of one hundred offending photographs in the same place at the same time gives rise to a single unit of prosecution pursuant to [Mass. Gen. Laws ch. 272,] § 29C" rather than one-hundred separate charges and convictions. Id. at 74. To support multiple prosecutions for possession of child pornography in compliance with the Double Jeopardy Clause, that possession must be "'sufficiently differentiated by time, location, or intended purpose.'" Id. at 73 (quoting Commonwealth v. Rabb, 431 Mass. 123, 130 (2000) (with internal quotation marks omitted)).

- Commonwealth v. Wassilie, 482 Mass. 562 (2019). The defendant, who was convicted on 15 separate indictments relating to secretly videotaping nude or partially nude adults and children, appealed, arguing that the judge erred in ruling that the proper units of prosecution were the individual victims rather than the individual episodes of surveillance. Id. at 563. The defendant concealed his cell phone in a unisex, one room bathroom without stalls at an angle that gave a clear view of the toilet. Id. at 563-564. He recorded two videos on the same day, and these videos captured "genitalia of children and adults, male and female"—a total of seventeen adults and five juveniles. Id. On appeal, the Court cited precedent that, for the purpose of determining whether particular conduct constitutes a single offense or multiple offenses, there are two categories of statutes. Id. at 567. "One category is focused upon the prevention of violence or physical injury to others." Id. In this category, a single incident can give rise to multiple indictments, based on the number of victims. Id. The other category is directed at "punishing the defendant for conduct offensive to society." Id. For this second category, separate indictments for separate victims are not appropriate. Id. at 568. Some crimes, like the one at issue here, do not fit neatly into either category. Id. The defendant argued that the statute reflects an intent to punish the physical act of recording, but the Court read the statute as punishing criminal acts that invade an individual's privacy. Id. The Court also rejected the defendant's reasoning on the grounds that his statutory interpretation would produce the "absurd result" of allowing people who take illicit photos of multiple people to be tried as if they had one victim. Id. at 571. Based on this statutory analysis, the Court upheld the lower court's decision to use a per victim unit of prosecution. Id. at 578.

2. Brief Possession is Sufficient

Brief possession of offending images is sufficient to sustain a violation of Mass. Gen. Laws ch. 272, § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 329–30 (2011). Evidence of prolonged or continued control is not needed. Id. (citing Commonwealth v. Harvard, 365 Mass. 452, 458 (1969)). In Hall, although the defendant's cell phone no longer contained child pornography and though there was no confirmation that the defendant had viewed the pictures sent to him by the victim, the defendant was

found guilty of possession of child pornography because the fact that he had enticed and encouraged the victim combined with the fact that he received the images allowed a jury to find that he had possessed them. Id. at 327–29.

3. Receipt by Cell Phone is Sufficient

Confirmation that defendant's cell phone received picture messages from the victim, where the defendant enticed the victim to take and send the picture messages, is sufficient to show control and possession of such photos in violation of Mass. Gen. Laws ch. 272 § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 327–29 (2011).

4. Malware and Computer Viruses Defense

The First Circuit notes that "we must be cognizant of 'the prevalence and sophistication of some computer viruses and hackers that can prey upon innocent computer users' by placing child pornography on their machines, but 'the specter of spam, viruses, and hackers must not prevent the conviction of the truly guilty.'" United States v. Rogers, 714 F.3d 82, 87 (1st Cir. 2013) (quoting United States v. Pruitt, 638 F.3d 763, 766–67 (11th Cir. 2011)). In Rogers, the possibility that the child pornography found on the defendant's computer was a result of malware was ruled out by forensic analysis (where an analyst installed the same malware on another computer and no child pornography was found) and corroborating evidence (child pornography found on another computer, browsing history matching an interest in child pornography, and evidence that some of the pornography had been deleted by the defendant). Id.

5. Probable cause / Staleness in Child Pornography Cases

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that the probable cause in the affidavit in support of the warrant to search his home was stale. Id. In Guastucci, police were investigating the upload of a single image of child pornography from the defendant's home to Skype seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time, the Court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the Court separately identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant

affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]", an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

B. Statutory Terms of Mass Gen. Laws ch. 272

1. "Dissemination"

"The definition of 'disseminate' includes 'publish, produce, print, manufacture, distribute, . . . exhibit or display.' The statutory emphasis is on the content of the material and the intent of the person disseminating such material; the draftsmen were not so much concerned with the manner in which the image was distributed, exhibited, or displayed. The statutes criminalize such dissemination whether accomplished by way of hand, mail, facsimile, or through the use of e-mail. The judiciary ought, absent constitutional inhibitions, give effect to the purpose of the law gleaned from the Legislature's choice of language." Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *2 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 31 (internal citation marks omitted)).

"Possession" is not an element of the crime of "dissemination." Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *4 (Sep. 22, 2016) (unpublished). To "disseminate" is defined as 'to import, publish, produce, print, manufacture, distribute, sell, lease, exhibit or display." Id. at *5 (quoting Mass. Gen. Laws ch. 272, § 31). In Moore, the appeals court held that "[t]o infer a requirement of possession would be to add a requirement not expressed by the Legislature." Id. The term "dissemination" also connotes some form of distributive act beyond showing something to another. Id. Consider Commonwealth v. McDonagh, 480 Mass. 131 (2018), where the defendant showed nude pictures on his computer to his minor son. The Commonwealth charged the defendant with various offenses, including dissemination of obscene matter (in violation of Mass. Gen. Laws ch. 272, § 29). Id. at 132. On appeal, the Commonwealth conceded that the evidence was insufficient to prove "dissemination." Id. at 144–45.

2. Computer "Depictions"

"The Legislature was unconcerned with how the photographically created image is stored or communicated." Commonwealth v. Hall, 80 Mass. App. Ct. 317, 326 (2011). "[T]he Legislature's creation of a separate and distinct category for 'depiction by computer' manifests an intent to give special treatment to the unique issues presented by computers, including the fact that stored data, although intangible in their unprocessed form, are readily transferrable to a graphic image." Id. at 327 (quoting Mass. Gen. Laws ch. 272, § 29C).

"Depiction by computer," as that phrase is used in § 29C, includes an unopened file on a hard drive—not only a file that is reduced to a hard copy, or one that is disseminated. Commonwealth v. Hinds, 437 Mass. 54, 63–64 (2002).

3. Child Enticement

"[I]n order to constitute enticement of a victim, the defendant need not physically meet the victim at the same place to which he entices the victim to go" given modern and electronic digital technology. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 323 (2011). In Hall, the Appeals Court noted that the defendant's enticement of the victim via cell phone text messages to go to a private place and take naked photographs to send to him can qualify as enticement. Id. However, given the potentially duplicative offense of posing a child in a state of nudity, the court held that the defendant must lure the child to a place of his/her choosing, not the victim's choosing. Id at 324–25. As this element was missing in Hall, the defendant's enticement charge was set aside. Id. at 325.

4. "Visual Material"

"The Legislature's objective of including a broad range of 'visual material' in its proscription is further demonstrated by Section 31's second sentence which provides: '[u]ndeveloped photographs, pictures . . . and similar visual representations or reproductions may be visual materials notwithstanding that processing, development or similar acts may be required to make the contents thereof apparent.' Thus, in determining whether an image is a 'visual material' within Mass. Gen. Laws ch. 272, the manner of its dissemination is insignificant. Whether further acts are required to make the image apparent to the naked eye, by, for example, keying a computer board, does not render the image any less a 'visual material.'" Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *3 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 29C).

5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31

The SJC examined the definition of "nudity" under §31 in Commonwealth v. Provost, 418 Mass. 416 (1994). In this case, the defendant took photographs of children in the pool and boys in the locker room. Id. at 417–18. One child struck different poses and his partially covered scrotal area was visible in two photographs. Several others showed the child displaying his bare buttocks ("mooning" the defendant). Id. at 418. The SJC provided the following analysis of the statutory meaning of "nudity": "The defendant claims that his activities do not fall within the ambit of § 29A(a). He first contends that the photographs do not depict a minor in a state of nudity within the meaning of, which defines 'nudity' as: 'uncovered or less than opaquely covered human genitals, pubic areas, . . . or the covered male genitals in a discernibly turgid state.' Although [the child] had his underwear on, in two of the photographs portions of his pubic and genital area are clearly visible. The statute does not require that the areas be completely uncovered. It is enough that a portion of the genital area is visible." Id. at 418 (quoting Mass. Gen. Laws ch. 272, § 31).

6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A

A "performance" under Mass. Gen. Laws ch. 272, § 29A "does not expressly or implicitly require the physical presence of 'one or more persons.' In view of the advances in technology, a violation of the statute may occur without the defendant's physical presence." Commonwealth. v. Bundy, 465 Mass. 538, 545 (2013) (finding the statutory definition of performance satisfied by victim masturbating facing a

camera attached to a device that, through an Internet connection, resulted in the image being broadcast to the defendant for him to view).

A "performance" occurs "before one or more persons" even when the only audience member is the person who enticed or encouraged the performance because to hold otherwise would circumvent the plain meaning of "one." Id. at 544.

7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A

Mass. Gen. Laws ch. 272, § 29A(b), provides in relevant part: "Whoever . . . hires, coerces, solicits or entices, employs, procures, uses, causes, encourages, or knowingly permits such child to participate or engage in any act that depicts, describes, or represents sexual conduct for the purpose of representation or reproduction in any visual material, or to engage in any live performance involving sexual conduct, shall be punished . . . ." (quoted in Com. v. Bundy, 465 Mass. 538, 539 n.2 (2013)). In Bundy, the jury was instructed as follows on a charge under this statute:

> [I]n proving [the element of live performance], the Commonwealth must establish beyond a reasonable doubt that it was [the defendant's] specific intent to solicit, entice, cause, or encourage [the victim] to engage in a live performance involving sexual conduct. In determining whether the defendant possessed such a specific intent, [the jury] may consider all facts and circumstances, including the defendant's acts and statements. The statute also permits the Commonwealth to establish alternatively that the defendant knowingly permitted [the victim] to engage in a live performance involving sexual conduct.

Id. at 542.

The meaning of "knowingly permit" was at issue in Commonwealth. v. Provost, 418 Mass 416 (1994). The defendant in Provost asserted that "the depiction of [a victim's] pubic area was unintentional and that, since [the victim] voluntarily struck the various poses without instruction, [defendant] did not 'knowingly permit' him to pose in a state of nudity." Id. at 419. The court rejected this argument and held that:

> The photographs themselves suggest that the defendant knowingly permitted [the victim] to pose with a portion of his pubic region and genitals exposed. He took a series of well-focused photographs at various points in the process of [the victim's] dressing. [The victim's] genital area is prominent in many of the photographs. The defendant admitted that he sometimes took photographs of nude boys for sexual gratification. There was sufficient evidence, therefore, for the judge to conclude that the defendant knowingly permitted [the victim] to pose in a state of nudity. Furthermore, the fact that the defendant continued to take the photographs as [the victim] struck different poses certainly supports the inference that he "encouraged" [the victim] to pose in a state of nudity.

Id. at 419.

8. Lewdness

In Commonwealth v. Rex, 469 Mass. 36 (2014), during a standard cell inspection prisoner Rex was found in possession of seven photographs of naked children. Id. at 37. The photos were from National Geographic, a sociology textbook, and a naturist catalogue. Id. The Court held that the indictment for possession of child pornography was properly dismissed because the children depicted were not in unnatural poses and their genitals were not the focus of the photo. Id. at 47. Thus the photos did not depict lewdness—just nakedness. Id. at 47–48. "It is well settled that nudity alone is not enough to render a photograph lewd." Id. at 44 (quotation omitted).

C. Special Conditions of Probation

Special conditions of probation can be unconstitutionally vague — facially or as applied — if they do not give fair notice to a defendant of the scope of prohibited activity. Commonwealth v. Ruiz, 453 Mass. 474, 479 (2009). A defendant "cannot be found in violation of probationary conditions that might have been intended or would have made sense, only of those that are unambiguous and of which he has notice," Commonwealth v. King, 96 Mass. App. Ct. 703, 710(2019) (citing Commonwealth v. Lally, 55 Mass. App. Ct. 601, 603 (2002)), and "ambiguities in probation conditions are construed in favor of the defendant." Lally, 55 Mass. App. Ct. at 603 (citing Commonwealth v. Power, 420 Mass. 410, 421 (1995)).

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography." Id., at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. The court found this sufficed to put the defendant on fair notice that possession of "explicit stories describing the rapes of young children" would violate his probation. Id. at 786-87. However, the court found that a reasonable person would not consider photographs of adults in their underwear or with their hands covering their genitals to be pornographic. Id. Therefore, they were not "so inarguably pornographic as to put the defendant on fair notice that he was violating probation by possessing them," where the photographs "depicted no sexual activity or nudity, and it [was] unclear whether the intent behind them was to arouse sexual excitement." Id. at 786.

  Commonwealth v. King, 96 Mass. App. Ct. 703 (2019). Defendant, who had pled guilty to possession of child pornography, was subject to special probation conditions which provided, in relevant part, that: "(3) The probationer shall not access any internet services from any handheld device (e.g., Palm Pilots, Blackberries, and mobile telephones)"; and "(4) The probationer shall not use, enter, visit, participate in, or remain in any online chat room, bulletin board service, message board service, social networking site or service (for example, Facebook.com, Twitter.com, Instagram.com), or any other online communication service, with the sole exception of electronic mail." Id. at 704. The discussion during the plea colloquy clarified the scope of these two conditions such that, in summary, the third condition prohibited any Internet access from

handheld devices, and the fourth condition prohibited the use of social media on any device (except email). Id. at 705. When read together, the two conditions appeared to permit non-social-media Internet access (including email) from non-handheld devices. Id. While on probation, the defendant accessed "images of young girls wearing scanty dance costumes in provocative poses" and annotated print-outs of these materials by hand with the girls' names, ages, information about their siblings, and smiley faces in some cases. Id. at 706. He accessed these and similar materials using search engines (e.g., Google) and Wikipedia on computers, and emailed some of them to himself. Id. at 705. While acknowledging that the defendant's conduct was "troubling," the appeals court held that "the evidence was insufficient to permit the judge to find that he violated special condition four," because "[s]pecial condition four did not prohibit the defendant from using the Internet generally, or downloading information from it." Id. at 710 ("the defendant cannot be found in violation of probationary conditions that might have been intended or would have made sense, only those that are unambiguous and of which he has notice.").

In dicta, the King court wrote: "with the benefit of appellate hindsight, one cannot help but ask whether special condition four should not have been written differently and, in particular, whether it should have expressly prohibited the defendant from using a computer to access images or information about children, whether via the Internet or otherwise." Id. at 710. Further, "recogniz[ing] both the importance and difficulty of drafting clear special conditions of probation, especially when they involve technology," the court suggested it would "be helpful to supplement existing sources with a set of model, nonbinding special conditions" "for sex offenders and those who use technology to commit crimes," among others. Id. at 711.

Special conditions of probation that refer to pornography may use the "common meaning" of pornography, and may prohibit constitutionally protected activity that may not be the basis of an independent criminal conviction. Hamilton, 95 Mass. App. Ct. at 787.

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography,." Id. at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. Defendant argued that under Free Speech Coalition, which held facially unconstitutional a statute that criminalized possession of "sexually explicit images that appear[ed] to depict minors" but were actually "created by using adults who look like minors or by using computer imaging," Ashcroft v. Free Speech Coalition, 535 U.S. 234, 239–40 (2002), the explicit stories he posessed were not pornography because they were "'fantas[ies]' that [did] not involve actual children." Hamilton, 95 Mass. App. Ct. at 787. The court rejected defendant's argument, noting "that a probation condition is enforceable, even if it infringes on a defendant's ability to exercise constitutionally protected rights, so long as the condition is 'reasonably related' to the goals of sentencing and probation." Id. (quoting Commonwealth v. Lapointe, 435 Mass. 455, 459 (2001)). The court was not considering a facial challenge to a criminal statute, but rather had to decide the question of "whether a reasonable person in the defendant's circumstances would have known that the stories constitute

pornography in violation of his probation conditions." Id. Thus, "[t]he discussion in Free Speech Coalition [was] not germane to that question because the common meaning of pornography is not limited to materials depicting actual people. For example, had the defendant been found in possession of computer-generated images of what appeared to be children engaging in sexual activity, he indisputably would have been in violation of his probation, even though Free Speech Coalition says that those same images cannot be the basis of a criminal conviction." Hamilton, 95 Mass. App. Ct. at 787.

IV. Expert Testimony About Technology

Expert testimony is ordinarily required when the subject of the testimony "is beyond the common knowledge or understanding of the lay juror." Commonwealth v. Sands, 424 Mass. 184, 186 (1997). Even if a juror does not have personal experience of a technology, a lay juror, from common experience and knowledge, may understand the required concepts when provided sufficient non-expert testimony and evidence. Commonwealth v. Bundy, 465 Mass. 538, 546 (2013) (finding the victim's testimony and photographic evidence sufficient to keep jurors from engaging in conjecture about an Xbox and its accessories) (citing Commonwealth v. Sands, 424 Mass. 184, 186 (1997)).

- Commonwealth v. Javier, 481 Mass. 268 (2019). In this first-degree murder case, the defendant argued, among other things, that the trial judge erred in admitting opinion testimony by a cell phone company employee interpreting CSLI information. Id. at 269. The defendant argued that the employee, who was not an engineer, should not have been permitted to testify about how cell sites operate and how to locate a cell phone based on historical cell site information. Id. at 277, 285. The SJC noted that it had previously expressed some doubt—in an appeal by the defendant's co-venturer, see Commonwealth v. Gonzalez, 475 Mass. 396 (2016)—about the propriety of the phone employee's testimony in two respects. Javier, 481 Mass. at 286. In particular, the SJC explained in Gonzalez that the employee's testimony "'that calls are 'typically' transmitted through the closest cellular site, and that a call from [a particular] address was unlikely to have been transmitted through [a particular cell site] . . . may well have required a witness with greater technical expertise.'" Id. (quoting Gonzalez, 475 Mass. at 412 n.37). The Javier Court also noted, however, that the employee "properly qualified his testimony and explained that, even where a particular cellular telephone was most likely to connect to the nearest tower, there were many reasons why that might not happen," and therefore "the fact that he did not know or investigate the reasons why particular calls had connected to particular towers did not prejudice the defendant." Id. at 286. The SJC concluded that, "while it might have been better practice to exclude evidence that was of little assistance to the jury and that possibly could have been confusing, the judge did not abuse her discretion in allowing [the phone employee's] testimony about certain aspects of the CSLI." Id. at 286–87. Moreover, the portion of the employee's testimony "concerning the reasons that cellular telephones connect to cell towers, and what he 'expected' a particular telephone would be most likely to do here, would not have had any impact on the jury's verdict." Id. at 287.

- Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *3 (2016) (unpublished). In an appeal from convictions for possession and dissemination of child pornography claiming ineffectiveness of counsel for failure to object to the testimony of the Commonwealth's digital evidence analyst and to request a Daubert-Lanigan hearing to challenge the reliability and the admissibility of his testimony, the Appeals Court found the claim unfounded. Id. at *3. The prosecution's case was based on evidence found on the defendant's laptop. Id. at *1. The AGO analyst connected the laptop's hard drive to a "write blocker"—thus preventing any data additions or removals—and then created a duplicate image of the drive with a program called Encase. Id. A search of the duplicate image resulted in the discovery of three (3) peer-to-peer file sharing programs: "(1) LimeWire (containing more than 900 videos and images of child pornography); (2) eMule (containing more than 400 videos of child pornography); and (3) Ares (containing several search terms consistent with child pornography)." Id. at *1 The AGO analyst also examined the browsing history, text messages, and photographs on the laptop and the defendant's cell phone to corroborate his ownership and exclusive use of the two items. Id. The court found that the Commonwealth presented a strong case at trial and that "the defendant [did] little more than offer [u]nsupported speculation that further examination of the reliability and the admissibility of the prosecution's expert testimony would have undermined the prosecution's case." Id. at *3 (quotation and citation omitted).

V. List of Cases Organized by Device/Evidence Type

This section provides a quick reference list of the cases that appear elsewhere in this Guide, organized by device or evidence type. Case descriptions are in the respective sections where they are discussed.

A. Cell Phone Searches

- Riley v. California, 134 S. Ct. 2473 (2014).
- Commonwealth v. Barillas, 484 Mass. 250 (2020).
- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020).
- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019)

B. Search of Computer Files

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014).
- Commonwealth v. McDermott, 448 Mass. 750 (2007).
- Commonwealth v. Kaupp, 453 Mass. 102 (2009).
- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished).

C. Email

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

D. CSLI, GPS, and Other Location Technologies

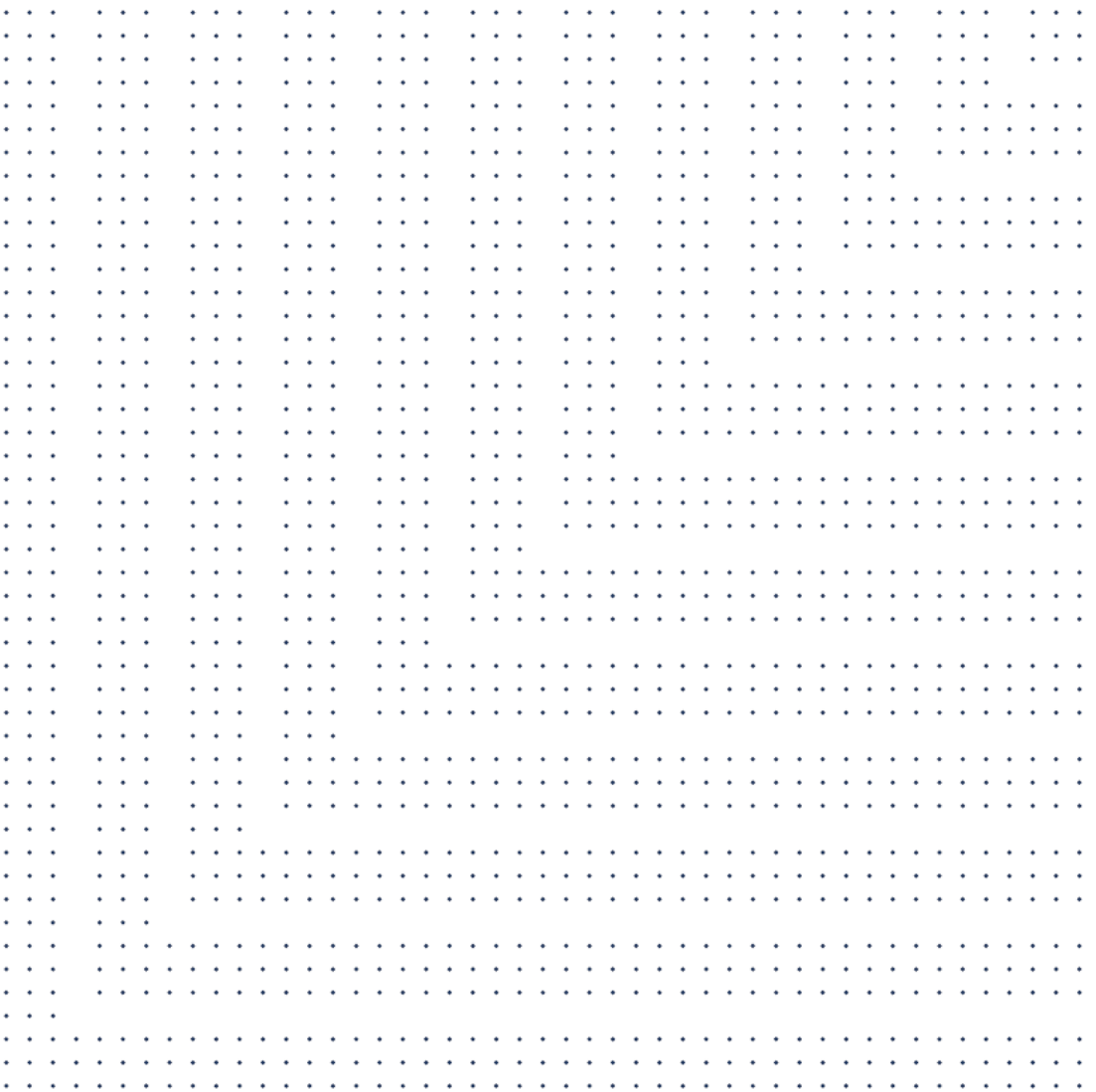
- Carpenter v. United States, 138 S. Ct. 2206 (2018).
- United States v. Jones, 565 U.S. 400 (2012).
- Commonwealth v. Gosselin, 486 Mass. 256 (2020).
- Commonwealth v. Wilson, 486 Mass. 328 (2020)
- Commonwealth v. Davis, 97 Mass. App. Ct. 633 (2020).
- Commonwealth v. Wilkerson, 486 Mass. 159 (2020).
- Commonwealth v. McCarthy, 484 Mass. 493 (2020).
- Commonwealth v. Mora, 485 Mass. 360 (2020).
- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020).
- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020).
- Commonwealth v. Vasquez, 482 Mass. 850 (2019).
- Commonwealth v. Hobbs, 482 Mass. 538 (2019).
- Commonwealth v. Fredericq, 482 Mass. 70 (2019).
- Commonwealth v. Lugo, 482 Mass. 94 (2019).
- Commonwealth v. Almonor, 482 Mass. 35 (2019).
- Commonwealth v. Feliz, 481 Mass. 689 (2019).
- Commonwealth v. Johnson, 481 Mass. 710 (2019).
- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018).
- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017).
- Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016).
- Commonwealth v. Estabrook, 472 Mass. 852 (2015).
- Commonwealth v. Augustine, 467 Mass. 230 (2014).
- Commonwealth v. Collins, 470 Mass. 255 (2014).

E. Text Messages

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.).
- Commonwealth v. Fulgiam, 477 Mass. 20 (2017).

Security Center AutoVu™

Automatic license plate recognition for public safety



Genetec™

Advancements in automatic license plate recognition (ALPR) technology have enabled police agencies worldwide to read thousands of plates effortlessly in each shift while improving the safety of those on duty. Choosing the right ALPR system is vital to ensure your officers apprehend more wanted suspects and recover more stolen vehicles.

Hardware

The SharpV and SharpX are designed to provide the most accurate plate reads even in bad weather, at poor angles and at high speeds. From vehicle mounted systems to fixed perimeter installations, AutoVu enables organizations to automate license plate identification, and share critical data amongst officers.



SharpV

- All-in-one device with on-board processing and illumination
- Power-over-Ethernet+ enabled device
- Plate capture up to speeds of 140 MPH (225 km/h)



SharpX

- Plate capture across three lanes of traffic
- Up to 5,000 plate captures per minute
- Plate capture at up to differential speeds of 200 MPH (320 km/h)

Software

Genetec™ Security Center & AutoVu Patroller connect to provide ALPR data to your office in the field and at the precinct to provide them with actionable information when responding to incidents.



Genetec Security Center

Security Center is a unified security platform that provides real-time monitoring of AutoVu events gathered from patrolling units in the field and from fixed AutoVu SharpV units. View video, reads and hits in dynamic maps, manage alarms, and generate advanced graphical reports in a single, versatile interface.



AutoVu Patroller

AutoVu Patroller is the intuitive, touch-based in-vehicle interface of the AutoVu system, providing easily accessible features for officers onboard, and allowing them to monitor incoming reads from ALPR cameras. With colour-coded and auditory notifications, your officer can safely know that vehicles of interest have been spotted without being distracted from the road.

5 reasons for choosing AutoVu



1 Highest accuracy in the industry

Backed by over 20 years experience in ALPR technology development, police agencies trust AutoVu to identify the most license plates within the camera's field of view. By combining state-of-the-art ALPR cameras and advanced software features, AutoVu provides officers with the best possible match of every license plate to maximize identification of vehicles of interest.

2 Ease of use

AutoVu is designed to automate and simplify the verification of license plates against multiple hotlists, and alert them when vehicles of interest are detected. AutoVu provides a user-friendly interface and features, including touch-enabled functions, graphical maps, associated image and time captures on every read.

3 Purpose-built, real-time surveillance

An ideal choice for police agencies requiring a field-proven ALPR solution, AutoVu users get real-time surveillance and identification of plates, while officers can also monitor the live ALPR information centrally using the Security Center client.

4 Deploy as a standalone or think bigger

AutoVu can easily be deployed as either a standalone system, or incorporated within a greater security or citywide surveillance environment. Through Security Center, cities and police agencies can manage and monitor their ALPR and video surveillance feeds, generate consolidated reports and centralize their alarm management.

5 Advanced reporting and data mining capabilities

When reviewing plate reads or receiving new vehicles of interest, officers can easily search for full or partial license plates from their vehicle. Operators can rapidly review each hit corresponding to searches, as well as any associated data, including geographic coordinates, context images and plate state when available.

AutoVu key features

Fuzzy matching

Fuzzy matching analyzes even imperfect or incomplete license plate reads, containing one or more errors, against a hotlist and alerts the officer case of any potential matches to optimize your patrol efficiency.

In-vehicle mapping

Accessible from within the vehicle or the backoffice, map displays provide operators an easier method to not only visualize the location of a read and correlate reads across multiple regions but also generates a specific location such as a street address.

Wildcard hotlists

When only partial license plate numbers are available to identify a suspect vehicle, officers can create a wildcard hotlist database in order to rapidly identify potential hits. Notifications of hotlist hits can be identified with different sounds, colors, and priority assignments than those of definite matches.

Covert hotlists

Covert hotlists allow you to ensure the discretion of an on-going investigation or special operation. When a hit is identified, only the authorized officer at the Security Center station will be notified, while the in-vehicle patroller will not be alerted. This enables enforcement officials to assign multiple objectives to the vehicle and backend systems, while not interrupting the priorities of officers on duty.

Automatic events and alarms

Officers can receive automated alarms and events from the AutoVu system when a black-listed, wanted, or stolen vehicle is detected. This allows officials to prioritize and rapidly respond to the incidents.

Live data transmission

The AutoVu system ensures officers are kept up-to-date with the latest information through the live update of ALPR reads and hits. Using the Security Center client, officers can remotely monitor one or more Patroller units, fixed SharpV cameras, and/or specific hotlists in real-time.

Third-party system integration

Through its advanced software development kit (SDK), AutoVu can integrate with other software applications to fit within existing workflows and operational processes.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2018. Genetec, AutoVu, the Genetec Logo, and the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

MCTCBR_BR1EN

BainCor, Inc.

763 South Street
Suite A
Holbrook, MA 02343

Estimate

Date	Estimate #
8/1/2022	2524

Name / Address
Massachusetts State Police Division of Homeland Security and Prepare Office of the Division Commander Framingham, MA 01702

Project

Description	Qty	Rate	Total
"Wanco" Model: WCTS-730 Trailer: Welded tubular steel construction, Extendable Rear Bumper for Added Wind Stability, Front access fork lift pockets, Round Full Wheel Fenders that are Bolted to the Trailer Frame, Axle Assembly 2,000 lb., Double-Eye Leaf Springs, 13" Wheel / tires, Four 2,000 lb. Corner Stabilizer Jacks, Red and White Conspicuity Tape Drawbar: Removable, 2" Ball Hitch, Swivel Wheel Tongue Jack, Flat-four trailer lights plug Tower: 20' telescoping tower with hand crank winch. Cable requirements required and/or supplied by others Solar panel: 730 Watt hand crank tilting frame, Solar charge controller 30A with LVD Batteries: Heavy-duty steel security box with dual puck locks, four 4D AGM Batteries (12Vdc system, 800 Ah Total Capacity), 45 Amp Smart Battery Charger, Master disconnect switch Standard colors: Powder-Coated safety orange frame, tower and battery box EMC-1 Module for Morningstar Solar Charge Controller MassDOT State Wide Contract INTF0000K03C00111753	[redacted]	[redacted]	254,700.00

MassDOT State Wide Contract
INTF0000K03C00111753

Subtotal	$254,700.00
Sales Tax (0.0%)	$0.00
Total	$254,700.00

This estimate/quote is valid for 30 days.

Phone #	Fax #	E-mail	Web Site
339-987-5525	339-987-5528	wbainter@baincor.com	www.baincor.com

The Commonwealth of Massachusetts
Department of State Police

Troop-H Communications
50 Massport Haul Road
Boston, MA 02110

Tel: (617) 946-3080 • Fax: (617) 946-0099

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

TERRENCE M. REIDY
SECRETARY

CHRISTOPHER S. MASON
COLONEL/SUPERINTENDENT

R. SCOTT WARMINGTON
DEPUTY SUPERINTENDENT

Wednesday, January 26, 2022

TO: Mr. Matthew Barstow; Director of Telecommunications
Mr. Kenneth Handfield; Director of Dispatch Services

FROM: Michael K. Slater; Public Safety Dispatcher III

SUBJECT: Troop-H Dispatch Personnel with Access to Flock LPR

Sir,

1. Per your email request, this date, the following is a list of Troop-H Dispatcher personnel who had access to the Flock LPR system along with access information:

Dispatcher	Username	Access Initiated / Offered	Access Given By:	Date Access Given:	Access How Frequently
TEEVENS, Richard E.	Richard.Teevens @pol.state.ma.us	Dispatcher Initiated Request	Tpr. Michael Clement	June 2021	For BOLO purposes
TILDEN, Charles S.	Charles.Tilden @pol.state.ma.us	Dispatcher Initiated Request	Tpr. Michael Clement	June 2021	For BOLO purposes
McDONOUGH, JOHN B.	John.McDonough @pol.state.ma.us	Dispatcher Initiated Request	Tpr. Michael Clement	June 2021	For BOLO purposes
MASSA, Tania M.	Tania.Massa @pol.state.ma.us	Dispatcher Initiated Request	Tpr. Michael Clement	June 2021	For BOLO purposes

Respectfully submitted,

Michael K. Slater, ID# C295
Public Safety Dispatcher III

Cc: file

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

TERRENCE M. REIDY
SECRETARY

The Commonwealth of Massachusetts
Department of State Police
Commonwealth Fusion Center
470 Worcester Rd
Framingham, MA 01702

CHRISTOPHER S. MASON
COLONEL/SUPERINTENDENT

R. SCOTT WARMINGTON
DEPUTY SUPERINTENDENT

August 18, 2022

Vicky Mboka-Boyer
Program Coordinator
Executive Office of Public Safety and Security
Office of Grants and Research
Homeland Security Division
10 Park Plaza, Suite 3720-A
Boston, MA 02116

The Massachusetts State Police Commonwealth Fusion Center (CFC) was awarded $750,000 in FFY2020 funding for grant FSHSP20CFC.

The award was set to expire on 6/30/2022 and you previously approved an extension until July 31, 2023. This will allow us time to procure the equipment being requested through this modification. The Commonwealth Fusion Center continues to enhance intelligence and information sharing initiatives while sustaining the baseline capabilities for fusion centers. The CFC also continues to provide technological solutions to promote enhanced intelligence and information sharing.

As of 8/18/2022, there is approximately $570,000 remaining unspent in the grant. The CFC respectfully requests a reprioritization of approximately **$567,703** in grant funds for the FSHSP20CFC grant. The need for this reprioritization is due to numerous factors including:

- training and seminars that were not held and/or completed remotely due to the pandemic
- two contracted cybersecurity positions which we have not found a suitable candidate for (the position remains posted and we continue to interview viable candidates as they apply)
- ACISS time and materials funds which were not needed as anticipated
- subscriptions that were procured elsewhere

We propose the following modifications with the remaining funds. The purchase of the below equipment will continue to promote intelligence and information sharing utilizing LPR trailers and cameras. This equipment is intended to upgrade and/or replace trailers and cameras which are nearing end of life. In addition, upgrades to I2 Analyst Notebook Software will allow us to support cybersecurity and other criminal investigations.

Please note that pricing is accurate as of the writing of this memo and may be subject to change by the time procurement occurs.

1. Approximately $254,700 –AEL 12TR-00-TEQP
   To purchase approximately [redacted] battery mounted solar trailers designed for mounting equipment such as License Plate Reader cameras.

2. Approximately $151,959.89 - AEL 04MD-01-CMRA
   To purchase License Plate Reader Cameras – LPR cameras can be used for multiple public safety issues including: ensuring the safety of special events, amber alerts, silver alerts, or investigations such as the opiate crisis. The cameras we propose to purchase with these grant funds will be temporarily fastened to a fixed object, for example, a telephone pole, a sign board or trailer.

3. Approximately $160,650 – AEL 13IT-00-DFSN
   To purchase I2 Analyst Notebook Software Upgrade to I2 Analyst Notebook Premium
   This software allows link charting, timelines, and social network analysis which can be used for cybersecurity and criminal investigations.

4. Supplies - AEL 21GN-00-OCEQ
   It is requested that any funds remaining after the above purchases are made be used to purchase supplies to support the grant.

The proposed reprioritization of grant funds for the FSHSP20CFC grant falls within the scope, purpose and intent of the programmatic objectives of this grant. I respectfully request approval of this reprioritization request. Please let me know if I can provide further information.

Respectfully submitted,

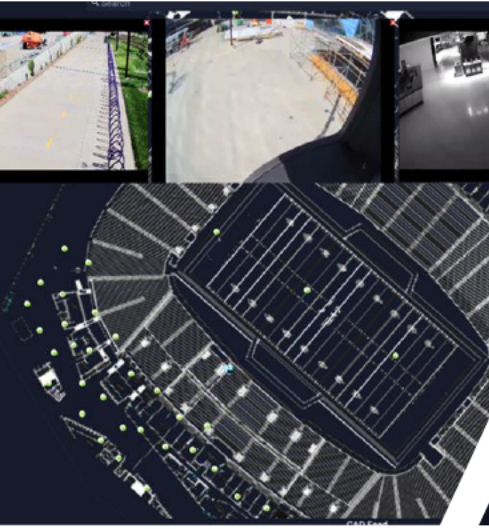
Amy Thibault
Intelligence Services Manager
Massachusetts State Police
Commonwealth Fusion Center

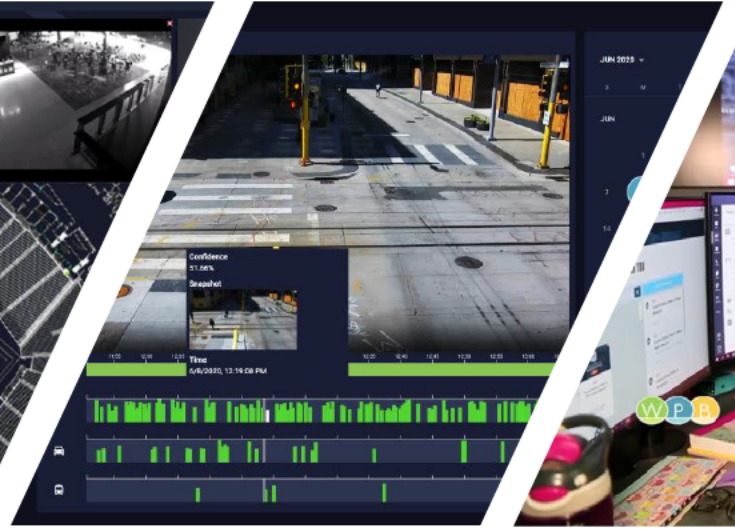


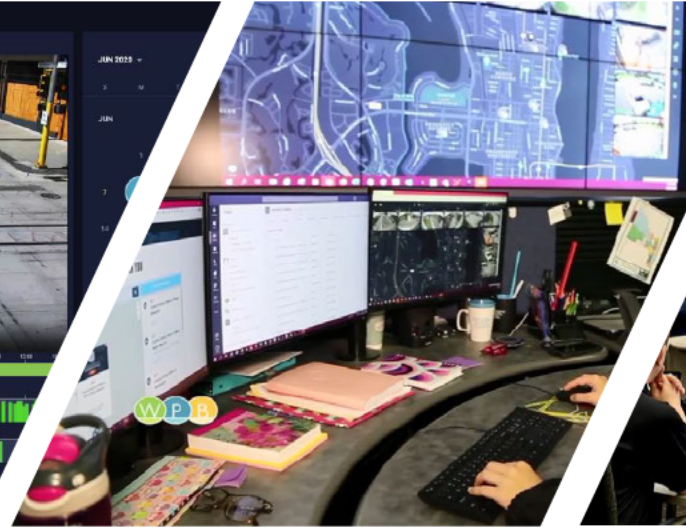
© Fusus 2021. Confidential- Not To Be Disseminated Beyond Original Recipient.

Fusus is the most widely used & trusted Real-Time Crime Center platform in U.S. Law Enforcement











POWER A REAL-TIME CRIME CENTER IN THE CLOUD.

- Integrate with any Data Source
- Pull in Public & Private Video Feeds
- Enable video sources with Artificial Intelligence
- Integrate Multiple ALPR Platforms
- Utilize & Unify all Existing Equipment





THE FŪSUS PUBLIC SAFETY ECOSYSTEM BRINGS IT ALL TOGETHER.

Real-Time Video Sources


Aircraft & Drone


Covert



Private Camera Feeds


Robot


City & Transit



Vehicle


Bodycam

IoT Triggers & Sensors


Panic Alerts



ALPR Integration


Indoor & Outdoor Gunfire Detectors


AI Weapons Detection



AI Sentry Search


Motion & Access Control

RTC 3
REAL-TIME CRIME CENTER IN THE CLOUD

Community Engagement & Evidence Collection


Multi-Media Public Tips


Emergency Mass Notification


Digital Evidence Vault with RMS Integration


Camera Registry

Operational Utilities & Communications


Intelligence/Operations Center


911/CAD


Unified Map of All Assets, Feeds & Personnel




Secure Chat Floorplans Telestration


Live Remote Viewing: Smart Phones/Tablets/MDTs



First Responders & Tactical Response Teams: Live Video Feeds & Geolocation

LEARN MORE ABOUT FUSUS.

(Click on video to view)



REAL-TIME CRIME CENTER IN THE CLOUD(2:02)

A Rapidly Deployable Solution.

Standard On-Prem System Deployment

(Time & Cost to Deploy Hardware Onsite, Third Party Installation/Resale/Engineering, Infrastructure Upgrades, Custom Engineering)

20 + Months

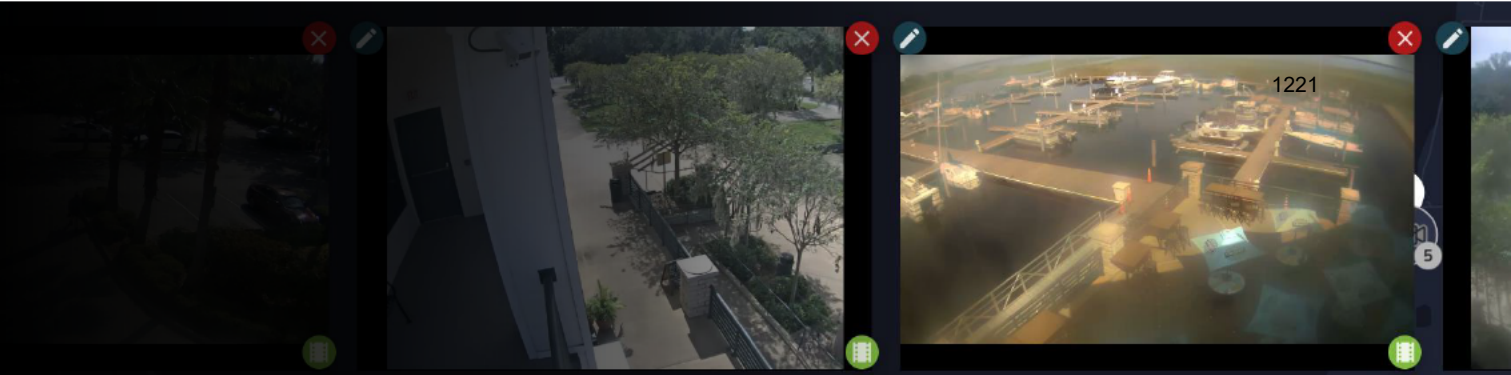
2.75 Months

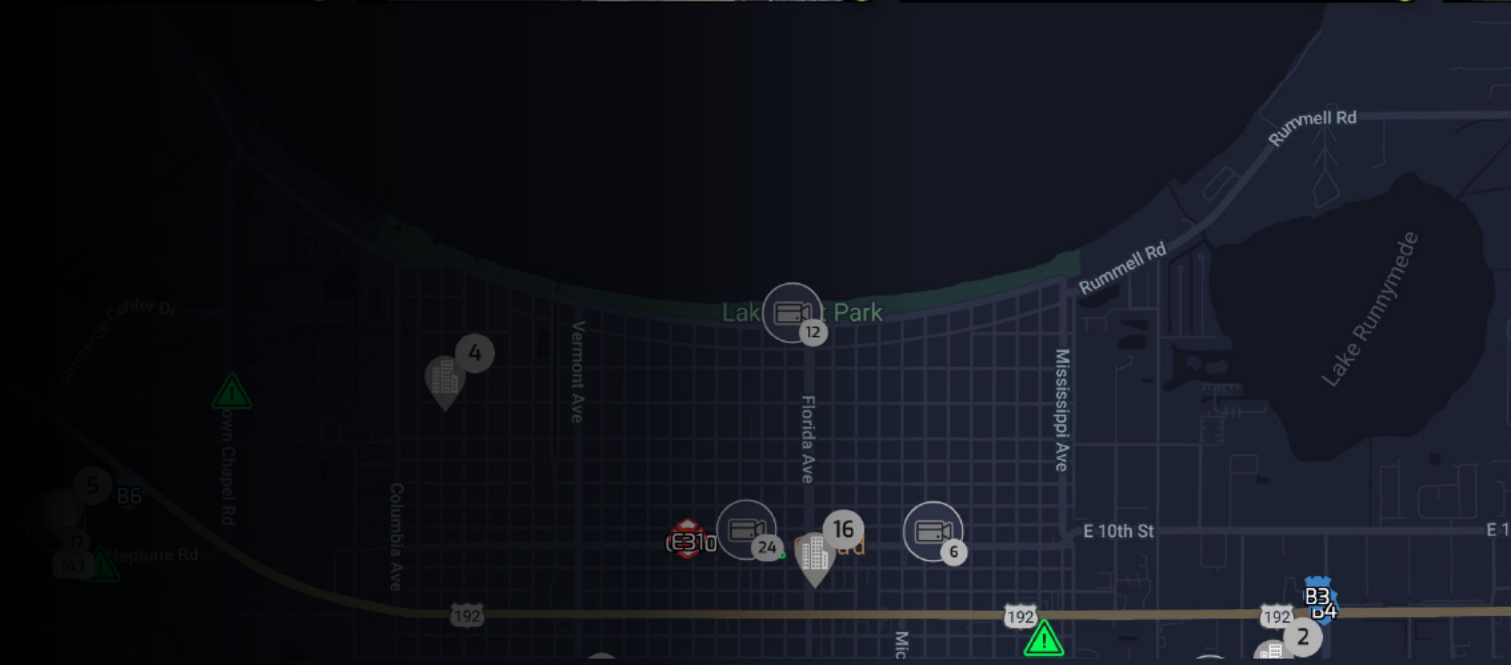
Fusus Real-Time Crime Center In The Cloud Deployment

(Rapid Deployment Over the Air)

fūsus ONE

- ✓ Streamlines Emergency & Incident Management, by Fusing all Community's Video Assets into a Single Platform.
- ✓ Enables Real-Time Crime Centers to Efficiently Gather Intelligence.
- ✓ Provides First-Responders with the Tools to Efficiently Monitor and Rapidly Respond to Evolving Situations.





St. Cloud Active Calls

Call type	Caller name	Caller phone	Assigned unit	Received time
SUPPLEMENTAL GENERAL CASE INFO	CARINO,MANUEL	4079244610		10/14/2020, 12:5
KEEP THE PEACE	MILLER VICTORIA	4078372815	A2	10/16/2020, 10:5

fūsus RTC 3

fūsus CORE

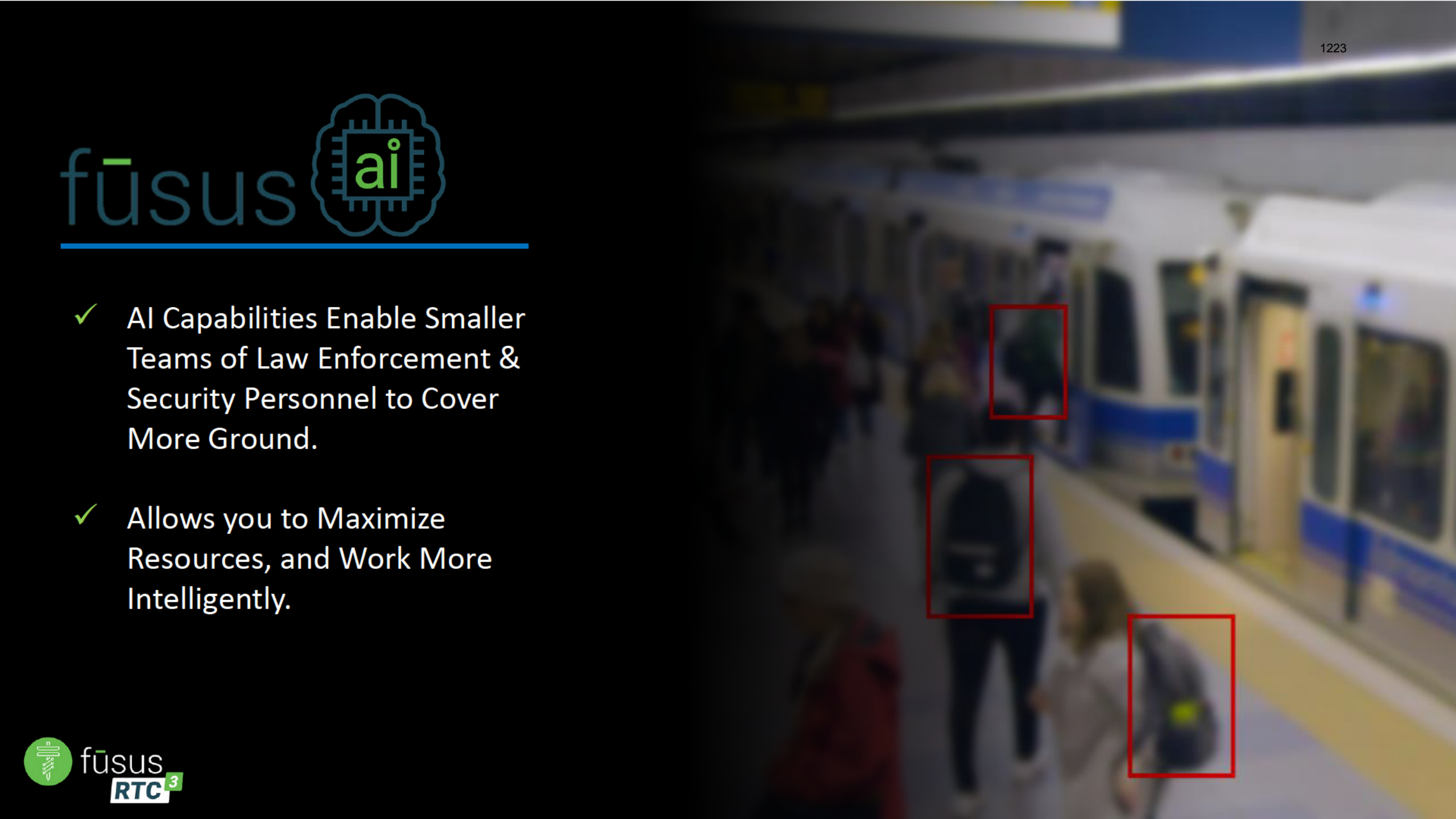
- ✓ Drop the fūsusCORE Appliance Onto any Public or Private Video Network and you Have Access to Live Streaming Video Feeds.
- ✓ The CORE Appliance is Compatible With a Wide Range of IP Security Cameras and is Controlled and Configured Remotely Using the fūsusONE Dashboard.



fūsus RTC 3

fūsus ai

- ✓ AI Capabilities Enable Smaller Teams of Law Enforcement & Security Personnel to Cover More Ground.
- ✓ Allows you to Maximize Resources, and Work More Intelligently.



fūsus RTC 3

fūsus OPS

- ✓ Enables First-Responders in the Field to Transmit their Location.
- ✓ Send Panic Alerts, Text Alerts and Send/Receive Images to Communicate Directly with the Command Center.
- ✓ fūsusOPS App is Available via iOS or Android Compatible Devices.



fūsus RTC 3

fūsus ANALYTICS

- ✓ Enables Law Enforcement to Unify Their Data and Operations Into a Single Platform.
- ✓ Facilitates the Correlation of Disparate Data Sources and Automates the Discovery of Trends.
- ✓ Augments Human Intelligence for Better Decision Making.



fūsus RTC 3

fūsus VAULT

- ✓ Streamlines Investigations with a Cloud-Based Digital Evidence Vault for the Secure Collection of Recorded Incident Video and Data, Including Public Tips.
- ✓ The Digital Evidence Vault is Easily Searchable and Enables Users to Cross-Reference and Group Evidence Related to the Same Cases, Speeding up Investigations.

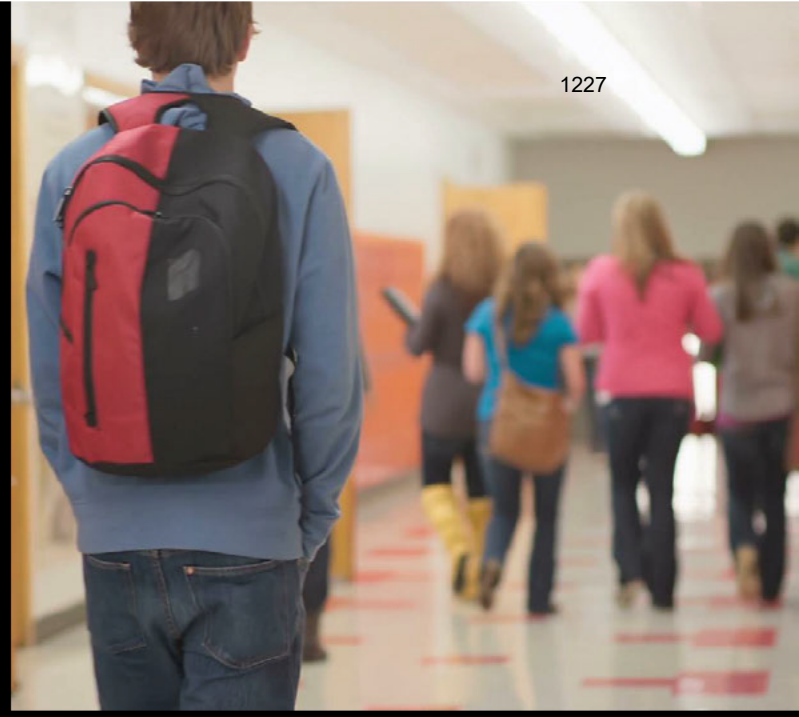
fūsus RTC 3



Fusus Community Connect.

- ✓ We Work With you to Engage Your Community and Assist you With Bridging the Gap.
- ✓ Our Goal is to Work With Your Agency and Make This Partnership Seamless.









fūsus REGISTRY

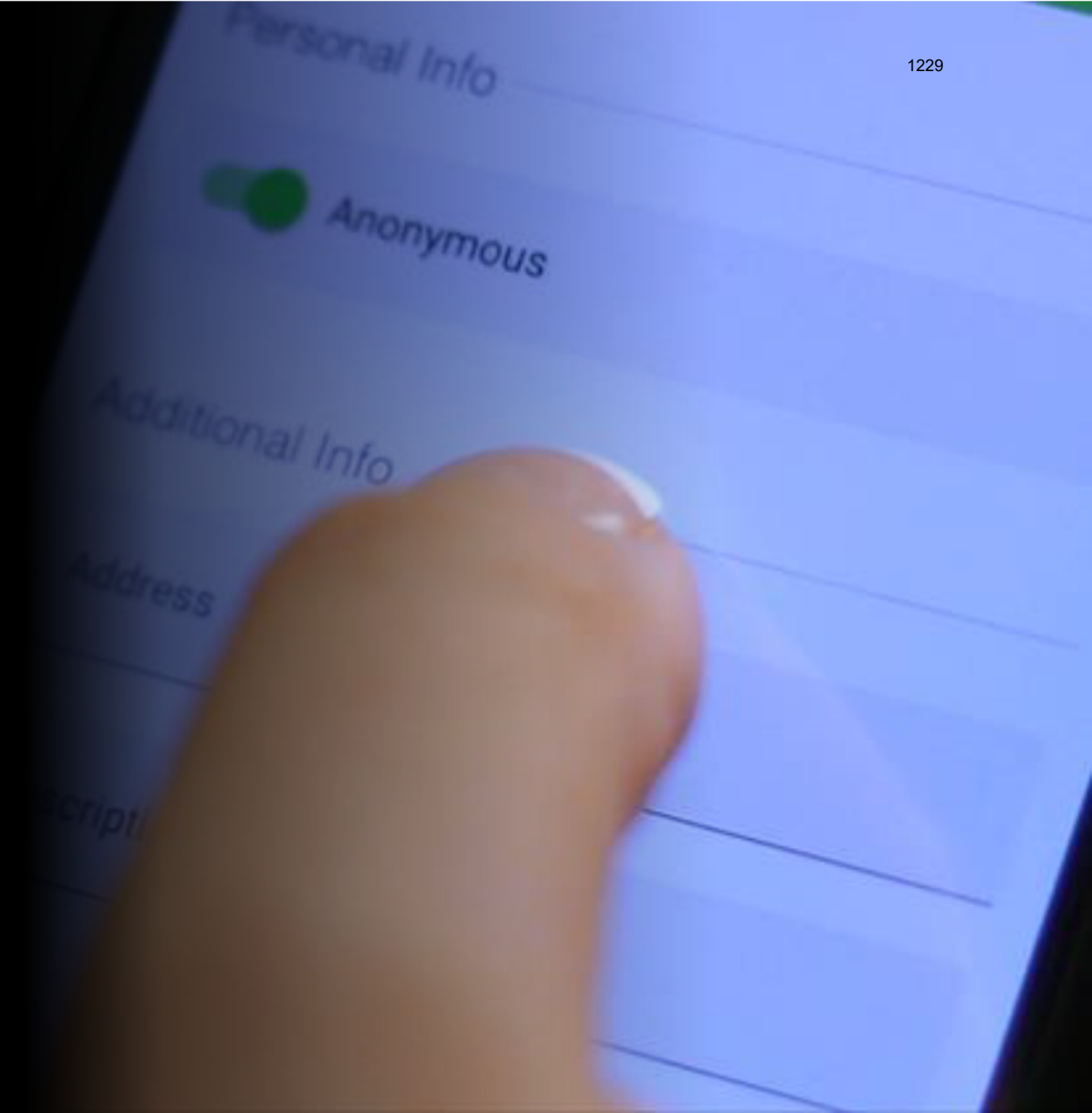
- ✓ Saves Time and Enables Investigations by Creating a Map of all the Public and Private Security Cameras in a Location.
- ✓ When an Incident Occurs, Investigators can use the fūsusREGISTRY to Easily Locate and Reach out to all the Camera Owners in the Vicinity and Request Video Footage.



fūsus RTC 3

fūsus TIPS

- ✓ Easy to use Public Safety Utility That Operates via Text Messaging.
- ✓ Members of the Public can Anonymously Submit Multi-Media Tips to the Police Department by Either Texting Information, Pictures, or Video to a Widely Publicized Number.
- ✓ Tips are Parsed Directly Into the fūsusVAULT Database for Examination.



fūsus RTC 3

fūsus NOTIFY

- ✓ Text Alerts can be Sent Directly via the FususONE Interface.
- ✓ Simply Choose to “Opt-In“ and That List of Community Members’ Cell Phones Will Receive the Alert.



fūsus RTC 3

TESTIMONIALS.



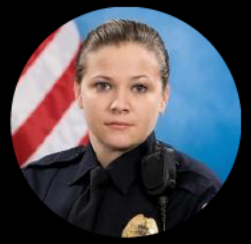
“Fusus technology and the team that supports the Division of Police's implementation have been nothing short of outstanding, and the program has been a game changer not just for the City, but I believe for law enforcement in general. Their team has continued to be extremely responsive and easy to work with, and their real-time intelligence platform is able to easily scale to meet our continuing needs. In addition to video surveillance sharing the Division of Police is in the process of rolling out the mobile FususOPS app to Specialty Units for Field Operations.”

Larry Jones II, Assistant Commissioner, Cleveland Department of Public Safety



"In an emergency every second counts. Our deputies need to gather information quickly and accurately. Fusus provides us real-time access to video, allowing us to gather intel to help speed up our investigations and response. This service allows us to have access to the cameras of businesses that opt-in. The archive footage is a huge advantage in latent investigations and is key evidence for successful prosecutions. We are grateful for this partnership that helps us keep our community safe.“

Sheriff Chad Chronister, Hillsborough County Sheriff's Office



“Fusus is extremely responsive to the agency needs and has demonstrated the ability to be on the cutting edge of technology. For example, our SWAT team asked for a certain feature and almost within a week, the capability had been developed. Overall, Fusus has been extremely easy to work with and understands the needs of law enforcement. The fact that Fusus is CJIS compliant is a big plus for most IT personnel and law enforcement concerned about cyber security.”

Lieutenant Amy Gauldin, Winston-Salem Police Department

LEARN MORE ABOUT FUSUS.

Visit the Fusus website to learn more about our platform.
https://www.fusus.com

Follow Fusus on LinkedIn to stay up-to-date with our latest news and insights.
https://www.linkedin.com/company/fusus-one/

Watch news videos and agency profiles to see how Fusus is being used.
https://vimeo.com/user107975383



© Fusus 2021. Confidential- Not To Be Disseminated Beyond Original Recipient.

MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES
GLOBAL JUSTICE AND PUBLIC SAFETY USER AGREEMENT

1.0 Purpose

This Global Justice and Public Safety User Agreement (hereinafter, "Agreement") establishes guidelines for the access, use, dissemination, and sharing of criminal justice information (CJI) collected and maintained within the systems and networks operated, maintained, and managed by the Executive Office of Public Safety and Security (EOPSS) and/or the Massachusetts Department of Criminal Justice Information Services (DCJIS).

2.0 Authority

This Agreement is established pursuant to M.G.L. c. 6, § 167A, M.G.L. c. 6, § 18 ¾, 803 CMR 7.00, and 28 C.F.R. Part 20.

3.0 Parties and designees

The parties to this agreement include EOPSS, DCJIS and the criminal justice agency noted in the signatory section below. The parties collectively agree to follow the terms of said agreement. EOPSS designates DCJIS as its designee with the authority to audit and provide oversight of Public Safety Data Enterprise Applications within the scope of the Agreement. Furthermore, EOPSS also appoints DCJIS as it designee to sign this Agreement on behalf of both DCJIS and EOPSS.

4.0 Scope

This Agreement is applicable to all sworn and non-sworn employees, contractors, interns, volunteers, and information technology support staff of all criminal justice and public safety agencies in the Commonwealth of Massachusetts who utilize or otherwise have access to any Public Safety Data Enterprise Application, software application, system or network maintained, or managed by EOPSS and/or DCJIS.

Public Safety Data Enterprise Applications within the scope of this agreement include the following:

Automated License Plate Reader (ALPR) technology is a system that allows for the automatic recognition of license plates by a portable or stationary unit. The license plate information is then compared against a locally stored list of plates called the CJIS-NCIC Hotfile database which consists of license plate numbers associated with suspended or revoked licenses, stolen vehicles, AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Be On Look Out, and Wanted or Missing Person broadcasts where a license plate is included.

CopLink is a crime analytics platform application maintained by the Massachusetts State Police Fusion Center that allows for the inter-agency storage and sharing of various documents and information.

EOPSS Data Cross Tracking System is a data collection and reporting system for criminal justice agencies and the Trial Court, to capture and report information on offenders and to report information relative to recidivism rates.

EOPSS National Incident Based Reporting System (NIBRS) Data Collection is a data

collection and reporting system that criminal justice agencies submit incident and arrest data to in compliance with the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) standards.

My License Office (MLO) is an application that allows for the retrieval and use of Massachusetts' driver's license photos for various reasons, including professional licenses and identification cards.

The **Victim Notification Registry (VNR)** is the electronic application that allows for the registration of crime victims to receive notification of an offender's release from incarceration and certain CORI information.

This agreement may be amended from time to time to update the listing of Public Safety Data Enterprise Applications within the scope of this agreement.

5.0 Duration of Agreement

This Agreement is in effect until modified or cancelled by EOPSS and/or DCJIS. Each Agency Head shall sign off on a copy of this Agreement as a condition of access to the systems and networks operated, maintained, or managed by the EOPSS and/or DCJIS. In addition, each Agency Head will sign off on a copy of the Companion System Agreement for each system for which such an agreement exists. An original, signed copy of this Agreement, along with original, signed copies of any Companion System Agreements, will be kept on file at the DCJIS. The Agency Head shall maintain a copy of the signed agreements. Facsimile and electronic signatures are acceptable as originals.

The Agency Head also agrees to execute a new Global Justice and Public Safety User Agreement and all relevant Companion System Agreements in accordance with 803 CMR 7.06 whenever there are changes to the Agency Head, the CJIS Representative , the backup CJIS Representative, or the CJIS Technical Representative. The new Agreement(s) is/ are to be executed within ten (10) business days of the effective date of the change(s) necessitating a new Agreement(s). Original, signed copies of the newly executed Agreement(s) will be forwarded to the DCJIS within ten (10) days of execution.

6.0 Definitions

Authorized User
A sworn or non-sworn justice or public safety employee, contractor, intern, volunteer, or IT support staff member who has been authorized by his/her agency head to access any software application, system, network, or CJI operated, maintained, or managed by the DCJIS.

Companion System Agreement
An addendum or "rider" to this Agreement. Each Companion System Agreement establishes rules and protocols for contributing CJI to, or accessing, using, or disseminating CJI from, a specific system or database operated, maintained, or managed by the DCIJS.

Criminal Intelligence System
A system that stores detailed intelligence or investigative information on the suspected criminal activities of subjects and/or which stores only information designed to identify individuals or organizations that are the subject of an inquiry or analysis.

Criminal Justice Information (CJI)
CJI is defined as all data obtained from or through the CJIS or companion public safety data enterprise application necessary for law enforcement agencies to perform their missions. CJI includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Information System (CJIS) Representative
The CJIS Representative serves as the primary agency point of contact for the DCJIS. Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS- sponsored meetings, seminars, and conferences.

Criminal Justice Information System (CJIS) Backup Representative
The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. The Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Rep representative be unable to perform those duties and responsibilities for any reason.

Criminal Justice Information System (CJIS) Technical Representative
The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

Criminal Justice Information System (CJIS) User-Access Model
A single-identity management model used to authenticate users of the software applications, systems, and networks operated, maintained, or managed by the DCJIS.

Public Safety Data Enterprise Application
A software application which criminal justice and public safety agencies use to contribute CJI to, or to access CJI from, databases or systems maintained by or accessed through the DCJIS.

Non-Contributing Agency
An agency that may access CJI from, but which does not contribute CJI to, a database or system operated, maintained, or managed by the EOPSS or DCJIS.

Source Agency
The agency that originally recorded and contributed data to a database or system operated, maintained, or managed by EOPSS or DCJIS.

7.0 Transaction Logs

An audit log of all transactions made by CJIS user agencies is maintained by the DCJIS and EOPSS for systems maintained by EOPSS or DCJIS. This log records the identity of the individual user and agency accessing the system, the date and time of access, and the data entered into, or retrieved from, any database or system operated, maintained, or managed by the EOPSS or DCJIS.
An Agency Head may request a report of all transactions initiated by the users of his/her agency. All report requests must be submitted in writing to the DCJIS.

The DCJIS CSO, at his/her discretion, may, at any time, authorize additional audits of all databases and systems operated, maintained, or managed by the EOPSS or DCJI S.

8.0 Audits of CJI Users

The DCJIS will conduct audits of all agencies, both criminal justice/public safety and non-criminal justice, accessing or using the CJI stored within, or obtained through, the databases, systems, and networks operated, maintained, or managed by the DCJIS. The purpose of these audits is to ensure the integrity and security of the CJI, applications, and systems, to investigate potential inappropriate use of these resources, and to identify potential training needs. Each CJIS user agencies will be audited at least on a triennial basis (once every 3 years).

9.0 Public Safety CJI, System, and Network Usage Restrictions

Use of any CJI obtained from or through an application, database, system, or network operated, maintained, or managed by the EOPSS or DCJIS is limited to authorized criminal justice purposes within the scope of a user's employment and official duties.

EOPSS and DCJIS resources may not be used for personal gain or for personal use, or to assist another individual or entity that is not authorized to access, use, or receive CJI from these resources. Criminal intelligence systems may also be subject to 28 CFR Part 23. Where the provisions of this Agreement or its addenda conflict with 28 CFR Part 23, 28 CFR Part 23 shall supersede this Agreement and its addenda.

10.0 Misuse

An Agency Head is responsible for investigating all alleged incidents or allegations of misuse of any CJI or database, system, or network operated, maintained, or managed by EOPSS or DCJIS. If an Agency Head determines that someone within his/ her agency has misused any of these resources, he/she must, within 10 business days, notify the DCJIS CSO in writing of the circumstances surrounding the misuse, of the actions taken, or to be taken, to address and correct the misuse, and of the policy(ies) and procedures to be implemented to prevent future misuse. The DCJIS CSO may suspend or revoke access to any or all databases or systems operated, maintained, or managed by the DCJIS for the individual(s) involved in the misuse.

Misuse of any EOPSS or DCJIS provided CJI or resource may result in individual loss of access to the resources, agency loss of access to the resources, and/or state and federal civil and criminal penalties, if applicable. Users are also subject to the rules and regulations of their respective agency.

11.0 Access to EOPSS and DCJIS Resources

Sworn and non-sworn justice and public safety employees, as well as the employees of non-criminal justice agencies, may be granted access to one or more DCJIS applications, systems, and networks as authorized by the Agency head.

Each individual accessing an EOPSS or DCJIS resource will be assigned a unique user identifier (User ID) and initial password. The individual will be required to change his/her password when logging into a resource for the first time. When possible, the same User ID and Password will enable a user to access multiple EOPSS and DCJIS resources. However, some applications may require a separate log in and/or a different User ID and Password.

All passwords used to access an EOPSS or DCJIS resource will meet the DCJIS and FBI security requirements in effect at the time the password is created/changed.

Authorized users shall not share their passwords and user identifications with any other individual. Each authorized user shall be responsible for all transactions conducted with his or her user identification and password.

Agencies are responsible for notifying the EOPSS or DCJIS, in writing, when a user is no longer authorized to access and EOPS or DCJIS resource. EOPSS or DCJIS will terminate or suspend user access depending on the user's status within his/her respective agency.

User IDs and passwords shall be reviewed by each agency on an annual basis. The Agency Head and agency CJIS Representative shall be responsible for this review. The purpose of this review is to confirm the continued authorization of all individuals accessing DCJIS resources. The Agency Head and CJIS Representative shall annually certify the accuracy of his/her agency's authorized user list to the DCJIS CSO.

12.0 Ownership of CJI Contained Within EOPSS or DCJIS Databases and Systems

The Source Agency will maintain ownership of, and responsibility for, the CJI it enters or modifies within any database or system operated, maintained, or managed by the EOPSS or DCJIS.

The Source Agency will exercise due diligence to ensure that the CJI it enters is current, complete, and accurate. Each Source Agency is also responsible for ensuring that the CJI it contributes is in compliance with all federal, state, and local laws.

User agencies shall communicate any errors found in CJI contained in any database or system operated, maintained, or managed by the DCJIS to the Source agency for that CJI as well as to the EOPSS or DCJIS.

13.0 Dissemination of CJI

CJI contained within, or obtained through, any database, system, or network operated, maintained, or managed by the EOPSS or DCJIS shall only be disseminated to other authorized agencies and individuals. In addition, the CJI obtained within, or obtained through, any DCJIS resource shall only be used for authorized criminal justice purposes.

14.0 Public Records

Records maintained within the databases and systems operated, maintained, or managed by the EOPSS or DCJIS are subject to the Massachusetts Public Records Law as defined in M.G.L. c. 4, s. 7(26).

All responses to public record requests for information contained in an EOPSS or DCJIS resource shall be referred to the Agency that contributed the relevant information for its response as the custodian of the record(s).

The EOPSS or DCJIS CSO may respond to a public records request for statistical data drawn from an EOPSS or DCJIS resource.

15.0 Data Submission and Retention Policy

Source Agencies shall contribute data to each EOPSS or DCJIS database or system pursuant to the schedule established in the Companion System Agreement for that database or system, if applicable. Companion

System Agreements are attached to this Agreement as Addenda.

Data maintained in an EOPSS or DCJIS database(s) and system(s) shall be retained pursuant to the schedule established in the Companion System Agreement for that respective system, if applicable.

16.0 Data Submission Standards

For each system that requires the contribution of data by Source Agencies, those Agencies shall submit at least the minimum set of data as established in the guidelines or any Companion System Agreement if required, for the respective subject application.

17.0 Designation of an Agency Representatives

CJIS Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the EOPSS or DCJIS shall appoint a CJIS Representative. The CJIS Representative serves as the primary agency point of contact for the EOPSS and DCJIS. Responsibilities include ensuring that all EOPSS and DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the EOPSS or DCJIS or who use the CJI obtained from or through those systems and networks, and attending all EOPSS or DCJIS- sponsored meetings, trainings, seminars, and conferences.

Backup CJIS Representative*:*
Each agency that accesses or uses CJI obtained from or through the syst ems or networks operated, maintained, or managed by the DCJIS shall also appoint a Backup CJIS Representative. The Backup CJIS Representative shall be the EOPSS and DCJIS' secondary point of contact for the agency. In addition, the Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

CJIS Technical Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Technical Representative. The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

18.0 Technical Support

The Executive Office of Public Safety and Security (EOPSS) Office of Technology and Information Services (OTIS) shall provide technical support services for all applications, databases, systems, and networks, operated, maintained, or managed by the EOPSS or DCJIS.

19.0 Internal Agency Policies

Each agency obtaining CJI either directly from, or through, an application, database, system, or network operated, maintained, or managed by the EOPSS or DCJIS shall draft and adopt internal policies to inform and ensure that agency authorized users have read and agree to comply with the provisions of this Agreement and its Addenda .

20.0 Termination of Access

An agency may request termination of its access to one or more EOPSS or DCJIS resources by providing a written request to the DCJIS CSO.
The DCJIS CSO may also terminate access to a DCJIS resource pursuant to the terms of a Companion System Agreement.

21.0 Amendments

Any change in the provisions of this Agreement or in the provisions of a Companion System Agreement shall be incorporated by a written amendment approved by the EOPSS and DCJIS CSO.

22.0 Global Justice and Public Safety User Agreement Signoff

By signing this Agreement, the Agency Head acknowledges he/ she has read and understood its provisions and that he/she will comply with its terms and conditions.

_____	_____
Agency Head Name/Title	Commissioner, Department of Criminal Justice Information Services
_____	
Agency	
_____	_____
Agency Head Signature	DCJIS Commissioner Signature
_____	_____
Date	Date

DEPARTMENTAL AND INTER-DEPARTMENTAL CORRESPONDENCE

City of Springfield

GO:	**16-03**	**DATE: 3-21-16**
TO:	**ALL COMMANDING OFFICERS**	
CC:	**DEPUTY CHIEF WILLIAM COCHRANE** **DEPUTY CHIEF MARK ANTHONY** **DEPUTY CHIEF ROBERT CHEETHAM**	
SUBJECT:	**AUTOMATED LICENSE PLATE READER (ALPR) SYSTEM**	

Table of Contents

I. Introductory Discussion
II. Policy
III. Acronyms and Definitions
IV. Procedures

I. INTRODUCTORY DISCUSSION

The use of the Automated License Plate Reader (ALPR) system will assist officers in the locating and investigation of vehicles whose license plate information is flagged in a national/state/local database. This system is intended to aid law enforcement in the timely recovery of stolen vehicles, investigations of missing persons and abducted children, and also to identify vehicles of interest in major crime investigations. This policy will further establish guidelines for the deployment and actions permissible when using the system.

II. POLICY

An ALPR system is a computer-based system that utilizes special cameras to capture license plate information. The ALPR system captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The text is compared to various hot lists generated by various law enforcement agencies, including the National Crime Information Center (NCIC) and the Springfield Police Department, and generates an alert when there is a hit. The ALPR system will identify a license plate and/or a motor vehicle. The ALPR system will not identify the person operating the motor vehicle. The Department may, as a separate step and for legitimate law enforcement purposes as set forth in this Policy, undertake to identify the owner of a vehicle in the event the ALPR system generates an alert, such as by running the license plate number through the database of the Massachusetts Registry of Motor Vehicles (RMV).

It shall be the policy of the Springfield Police Department that all department members abide by the policy and procedures set forth when using ALPRs to scan, detect, and identify vehicles or persons of interest, thereby increasing the efficiency and effectiveness of its public safety efforts in a manner that safeguards the privacy concerns of law-abiding citizens.

The ALPR system shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety. Such uses and goals include, but are not limited to providing information to officers that will assist in on-going criminal investigations, crime prevention, crime detection, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and improving the quality of life in our community through

the identification and removal of stolen, unregistered and uninsured motor vehicles, and enforcement of certain parking rules and regulations.

The Department shall utilize hot lists that further the above-specified goals of the ALPR system where there is legitimate and specific law enforcement reason for identifying a vehicle or a person reasonably believed to be associated with the vehicle, such as: persons who are subject to an outstanding arrest warrant; missing persons; AMBER Alerts; stolen vehicles; vehicles that are reasonably believed to be involved in the commission of a crime; vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list; vehicles with expired registrations; persons who are subject to a restraining order issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements; persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity; and persons who are on any watch list issued by a State of Federal Agency responsible for homeland security when information has been received concerning a specific individual or individuals who pose a potential public safety risk to the Springfield area.

In summary the ALPR system will aid officers in ensuring the safety of our community.

III. ACRONYMS AND DEFINITIONS

"Alert" shall mean a visual and/or auditory notice or alarm that is triggered when the ALPR receives a potential hit on a license plate.

"**Alert Data"** shall mean information captured by an ALPR relating to a license plate that matches the license plate on a hot list.

"**ALPR"** shall mean automated license plate reader.

"**ALPR Data"** shall mean scan files, alert date and any other documents or other data generated by or through utilization of the ALPR system.

"**ALPR System** shall mean the ALPR cameral and all associated equipment and databases.

"Hit" shall mean a read matched to a license plate that has previously been registered on an agency's vehicle plates hot list, such as those associated with vehicles that have been stolen or that are unregistered or uninsured, vehicles wanted for specific crimes, vehicle associated with, or that may assist with the identification of, suspects involved in criminal activity, and vehicles associated with parking scofflaws.

"**Hot-List"** shall mean data bases containing lists of license plate numbers of interest.

"**Non-Encounter Alert"** shall indicate to officers "Do not stop the vehicle based on this information alone". Only observe and report pertinent information to the requesting agency.

"OCR" shall mean optical character recognition.

"Read" shall mean digital images of license plates and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the ALPR system.

"**Scan File"** shall mean data obtained by an ALPR of license plates that were read by the device, including potential images of the plate and vehicle on which it was displayed, and information regarding the location of the police cruiser at the time of the ALPR read.

IV. PROCEDURES

A. Management

The Springfield Police Department, by and through its Police Commissioner, is solely responsible for the day-to day operation and management of the ALPR system and for all tasks ancillary to its operation and management. The Commissioner shall assign Department personnel to operate and manage the ALPR system on a day-to-day basis. The Commissioner or his/her designee may assign civilian personnel to perform any function or duty related to the operation and management of the ALPR system, including but not limited to, inventory, service and maintenance work.

The Commissioner shall ensure that the ALPR system is operated in conformity with this Policy and other Department policies, procedures, rules and regulations. The Commissioner shall enforce this Policy and shall act as the Department Head for all disciplinary and enforcement actions for any violations by Department personnel.

B. Operation

1. Installation and Functioning: The ALPR cameras will be mounted on a marked or unmarked cruiser or on fixed position locations in the city as determined by the Police Commissioner. The cruiser will engage in either directed patrol or routine patrol depending on the assignment given. The ALPR equipment will passively read the license plates of moving or parked motor vehicles using ALPR optical character recognition technology and compare them against various hot lists uploaded or created by the Police Department. Scanned data files collected by an officer will on an ongoing basis, be automatically uploaded from the ALPR in the cruiser to the Executive Office of Public Safety and Security (EOPSS). The ALPR system will not have sound recording capability.

2. Hot Lists: Designation of hot lists to be utilized by the ALPR system shall be made by the Commissioner or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in the Policy, which sources may include:

    a. NCIC Stolen Vehicle Files, as available;
    b. NCIC Stolen Plates and Stolen Canadian Plates, as available;
    c. NCIC Wanted Persons, as available;
    d. NCIC Missing or Endangered Person Files, as available;
    e. NCIC Supervised Release (Federal Probationers), as available;
    f. NCIS Nationwide Domestic Violence Protection Orders, as available;
    g. NCIC Violent Gang and Terrorist Organization File, as available;
    h. NCIC Sexual Offender;
    i. RMV Records of Suspended/Revoked Registrations;
    j. SPD Tow/Hold List;
    k. City of Springfield Parking Permit System; and
    l. Department –generated hot list(s) or manual entries of license plate numbers to existing hit list(s) created for purposes consistent with this Policy as may be authorized by the Commissioner or his/her designee.

    The Department shall regularly upload hot lists utilized by the ALPR system so that these hot lists remain reasonably current.

    Whenever a license plate number is manually entered into the ALPR system, the officer shall document the reason for doing so in the ALPR query screen.

3. Regular Operation: The Commanding Officer will assign as staffing permits, all available ALPR equipped vehicles for patrol.

4. Login/Log-Out Procedure: To ensure proper operation and facilitate oversight of the ALPR system, officers assigned to the ALPR vehicle shall login at the beginning of shift and log out at the end. Officers shall insure the system remains operational during their tour of duty.

C. Authorized Usage/Police Action

1. Authorized Users/Access: Only sworn officers and authorized civilian employees may operate the ALPR system or access or use stored ALPR data. Each authorized officer or civilian employee shall be issued an individual log-in ID and be required to utilize alphanumeric passwords consisting of a combination of upper and lower case, numbers and symbols.

2. Permitted/Impermissible Uses: The ALPR system is the property of the Springfield Police Department. Department personnel may only access and use the ALPR system and may access, use, release and/or disseminate hot list and scan file data only for official and legitimate law enforcement purposes consistent with this Policy.

The following uses of the ALPR system are specifically prohibited:

a. Invasion of Privacy**:** Except when done pursuant to a court order, it is a violation of the Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g. vehicle on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

b. Harassment / Intimidation: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists to harass and/or intimidate any individual or group.

c. Use Based on a Protected Characteristic: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists solely because of a person's race, gender, ethnicity, sexual orientation, disability or other classification protected by law.

d. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.

e. First Amendment Rights: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for the purpose of infringing upon First Amendment Rights.

Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to:

- criminal prosecution,
- liability, and/or
- administrative sanctions, including termination, pursuant to and consistent with the relevant collective bargaining agreements and department policies.

3. Required Steps Preliminary to Police Action: Hot lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them, and the Department's ALPR system will not have access to real time data. Further, there may be errors in the ALPR's read of a license plate. Therefore, an alert alone shall

not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, an officer shall undertake the following:

a. Verification of Current Status on Hot List: An officer must receive confirmation, from a Springfield Police Department Dispatcher or other Department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding.

b. Visual Verification of License Plate Number: Officers shall visually verify that the license plate on the vehicle of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate and the state of issue, before proceeding.

4. Stops: All stops of motor vehicles must be constitutionally valid and otherwise comply with the Department's Policy on Stop and Frisk and Threshold Inquiry. To assist with implementation of these obligations and in furtherance of the purpose of the ALPR system, the following requirements apply to traffic stops:

a. Completion of Preliminary Steps to Police Action: An officer must have Compiled with Section IV (C) (3) of this Policy prior to proceeding with a motor vehicle stop.

b. Non-Encounter Alerts: In the event that an alert is designated as a non-encounter alert, the officer shall follow any instructions included in the alert (e.g., notifying any applicable law enforcement or homeland security agency).

c. Persons of Interest: With regard to cases in which an alert may indicate a person of interest (such as a wanted person), officers are reminded that in some cases, the driver or occupant of the vehicle may not be the person with whom the license plate is associated (since vehicles may be loaned, e.g.). Therefore, officers must develop a reasonable belief that the operator or occupant is the person of interest included in a hot list prior to initiating a stop (e.g., by comparing the person's observed physical appearance with that of a physical description contained in the RMV database).

d. Independent Reason For Traffic Stop: An officer may stop a vehicle where he/she has an independent reason for doing so, such as an unrelated traffic violation.

e. Appropriate Police Action: Nothing in the Policy shall restrict or prohibit an officer from taking appropriate police action based on facts or reasons obtained independently from ALPR operation.

5. Use in Connection With Serious Crimes/Incidents: The ALPR should be considered to conduct license plate canvasses in the immediate wake of any homicide, shooting, robbery, kidnapping, sexual assault or AMBER ALERT and or other major crime or incident. Registration plates or partial plates potentially associated with any such major crimes or incidents

should be entered into the ALPR and compared against the scan file. Conversely, registration plate numbers may be used for exculpatory purposes (e.g., to corroborate a registrant's alibi).

6. Mutual Aid Requests: The Commanding Officer may approve a mutual aid request for use of the ALPR for purposes consistent with this Policy, as may be appropriate under the circumstances and as resources permit. Commanding Officers are encouraged to provide mutual aid to other communities when they become aware of a serious incident, as to which serious incident they reasonably believe the ALPR may be useful. Examples of serious incidents include homicides, shootings, kidnappings, sexual assaults or AMBER ALERTS, or other serious or violent felonies as to which suspect vehicle information is available. ALPR data may be shared under this Section IV (C) (6) only as is consistent with this Policy and to the extent necessary to supply duly approved mutual aid.

D. Security/Authorized Stored Data Access/Confidentiality:

ALPR data shall be kept in a secure data storage system with access restricted to authorized persons only.

a. Scan Files: Access to scan files will be secured and controlled by a login password-accessible system, which shall document who accessed the information by identity, date and time. Officers may only access data stored in the ALPR server based upon a reasonable belief that the scan file data may be related or useful as part of a specific official action or investigation. Requests for ALPR server data access must be in writing and be expressly authorized by the Police Commissioner, or designee(s), in advance of such access. Scan file data will be considered confidential information to the extent permitted by law.

b. Hot Lists: Security of the hot list data will be the responsibility of the officer using the ALPR or accessing the data. Hot list data will be considered confidential information to the extent permitted by law.

c. Designated Trained Officers: Officers trained in the use of ALPR software shall have access to ALPR data to conduct analysis of said data in order to comply with legitimate law enforcement requests.

E. Retention:

Scanned data files are transmitted to the ALPR server located at the Executive Office of Public Safety and Security will be deemed to be under their jurisdiction and time frame protocols. The Springfield police department will not retain scanned files or records.

F. Program Oversight/Evaluation/Audit Review:

1. Authorized personnel shall check equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected. Officers shall not attempt to modify or change the ALPR equipment or software unless authorized to do so.

2. Inoperability, damage or other malfunctions to the equipment shall be documented in a written report and will be immediately reported to the Commanding Officer.

3. All successful uses of the ALPR shall be documented and forwarded to the Commanding Officer of the Information Technology Division or his/her designee. The Commanding Officer or designee will then compile statistics of these uses and provide monthly updates on such uses to the Police Commissioner.

4. The Information Technology Division will be responsible for conducting, reviewing and retaining audits of the ALPR system usage. Audits shall be completed on a semi-annual basis and shall determine the Department's adherence of the Policy and the procedures it establishes, as well as the maintenance and completeness of records contemplated by the Policy. At the completion of this audit, a full report on the outcome shall be forwarded to the Police Commissioner. Audit reports shall be considered to be public record to the extent consistent with the Public Records Law. Audits shall include, but not be limited to, review of the following.

    a. Records of ALPR operators and their ALPR usage, including vehicles of interest added to a hot list by individual officers.

    b. A listing of access to the Police Department's server, to include access, additions and/or searches of the scanned files, in order to verify security of that data and compliance with this Policy. All written requests for scanned file access will be retained for comparison against this audit record.

    c. Records of sharing ALPR data pursuant to Section IV (C) (6) of this Policy.

    d. Records of reproduction of scan files pursuant to Section IV (G) below.

    e. Hot lists entries shall be checked to ensure entries made are in compliance with this Policy.

5. Any officer becoming aware of a possible violation of this Policy, including but not limited to the unauthorized access, use, release and /or dissemination of ALPR data, shall refer the matter for an Administrative Investigation to the Police Commissioner.

G. Requests for Reproduction of Scan Files:

1. Authority to Request/Permissible Requests: Sworn Department personnel of the rank of Sergeant and higher are authorized to make a request to the Information Technology Division for a reproduction of scan files. Requests for reproduction 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 this Policy.

2. Prompt Request: All requests to reproduce a scan file shall be made promptly and in any event as soon as possible to ensure that needed data is available.

3. Reproduction Responsibility/Evidence: The Department's Information Technology Division shall be responsible for making reproductions of scan files. It shall make two copies of any reproduction. One copy shall be logged into the evidence system following the Evidence Policy and with maintaining the chain of custody for evidentiary materials. The second copy shall be reproduced to the requesting party utilizing the procedure described in Section IV (G) (4) below. The Information Technology Division shall document all requests for copies of scan files.

4. Reproduction Request Procedures:

    a. Authorized Department Requests (see Section IV (G) (1) above):

By submitting a completed Scan File Request Form (available on the "in-house" web-site) to the Information Technology Division (cc to the appropriate Department Division (e.g., Detective, Traffic or personnel for follow-up). Department personnel of the rank of Captain or higher may authorize disclosure of a copy of scan files to any federal, state, or municipal law enforcement agency in connection with an open investigation.

b. Court-Related Requests (e.g., Prosecutors, Defense Attorneys, Judges):
By submitting a completed Scan File Request Form to the court liaison (for the applicable court), who shall forward a copy to the Information Technology Division. The Information Technology Division shall send a copy of the requested reproduction to the court liaison, who shall send it to the requesting party.

c. Subpoena:
Except in connection with an open investigation as set forth in Section IV (G) (4)(a) above, by submitting a completed Scan File Request Form to the Department's Office of Information/Keeper of Records, with the responsibility for reproduction falling to the Information Technology Division.

d. Public Records Requests for Scan Files:
Scan files shall be considered to be non-public record to the extent consistent with the Public Records Law.

John R. Barbieri
Police Commissioner

JRB/

Dispatch Services Unit
ALPR Guidelines

Purpose:
To support the Dispatch Services Unit with the identification and broadcast of real-time public safety information to State Police assets in exigent or urgent situations by providing guidelines for interaction with ALPR systems and access to authorized DSU supervisors.

Search Criteria:
Authorized:
- Public safety matters investigated by or relevant to MSP, such as:
  - Missing person, kidnapping, endangered elderly, suicidal subject, etc.
  - Vehicle fleeing from a crime or involved in a pursuit
- Allowed search time period: up to **24 hours**

Unauthorized:
- Investigative historical queries or searches for outside agencies
- Vehicles not associated with an active, urgent public safety matter
- Non-official purposes or to violate any constitutional or civil rights

Hotlist Entries
- Requested through the Commonwealth Watch Center by email
- Public safety matters investigated by MSP only
- No requests for outside agency matters; the agency may request directly to CWC
- Shall be updated or removed by the requestor when no longer valid
- Expire the following day (approx. **24 hours)**
- Extensions may be requested by the investigating unit directly to CWC

Radio Guidelines
- Avoid broadcasting non-timely information (i.e., reads that are not recent or relevant)
- Avoid broadcasting law enforcement sensitive information (i.e., source of information and specific device locations)
  - *Example terminology:* "We have received information that…"

Outside LPR Systems
- No accounts or direct access to outside or third-party ALPR systems
- Searches, hotlists, and radio broadcasts shall conform to these guidelines

Contact for Assistance:

Commonwealth Watch Center
(508) 820-2233 fusion@pol.state.ma.us

Refer to General Order TRF-11 for Additional Guidance

September 2022

1250

Criminal Search $1 00
Bankruptcy Search: $0.25
Motor Vehicle Search $0 50
Employment Search: $0.25
Locate Report $0 50
Property Search: $0.25
Deceased Search No charge
Reverse Phone Search: $0.50
Reverse IP Address Search $0 25
Reverse Email Search: $0.25
Liens Search $0 35
Judgments Search: $0.35
Comprehensive Report $5 00

NOTE We are continually adding additional data searches and reports You will receive notification of additional features and associated pricing prior to any new product release. You will receive advance notice to any changes to transactional pricing.

No hit, no fee! Searches that produce zero search results will not incur charges.

If you are a term agreement customer, please refer to your pricing agreement for details. If you would like to discuss a term agreement for further discounts, please contact your Sales Representative

IDI
www ididata com
idicoresupport@ididata.com
888 214 9509



L5F FIXED LPR CAMERA SYSTEM

SEE FARTHER. SEE CLEARER. SCAN MORE.

Missed scans mean unsolved cases and unrecognized revenue. The L5F Fixed License Plate Recognition Camera System captures clearer images at greater distances on your high-speed, high-volume roadways. Paired with Vigilant PlateSearch or Vigilant ClientPortal, this solution enables you to receive real-time alerts, conduct comprehensive searches and leverage advanced analytics and parking tools to uncover new vehicle location insights that protect communities and generate revenue.

KEY BENEFITS

Scan More Than Before
Capture your clearest plate detections yet, at greater distance, on your most high-volume, high-speed roadways.

Rely On Better Basics
Beyond ensuring you've captured the best data, we make management, alerting and searching straight-forward.

Do More With More Data
Use patented analytics, specialized tools as well as easier data sharing and access to derive new intelligent insights.



MOTOROLA SOLUTIONS

L5F FIXED LPR CAMERA

The L5F Camera features a new state-of-the-art sensor that allows it to capture clearer images at greater distances on your high-speed, high-volume roadways.



CAMERA PERFORMANCE

Part Number	Optimal Focal Length	Capture Range*
VSR-5x-908	14 ft	6-27 ft
VSR-5x-916	40 ft	25-55 ft
VSR-5x-925	70 ft	55-85 ft
VSR-5x-935	95 ft	85-105 ft
VSR-5x-950	115 ft	105-125 ft

*Up to 2 lanes of traffic coverage in most scenarios.

OPTICS

Window	Shatterproof window	
Resolution	1440x1080 Monochrome global shutter	1440x1080 Color global shutter
Capture speed maximum	150 mph (241 kph)	

ILLUMINATION

Pulsed LED illumination	Zero lux environments *850nm and 750nm options

VIDEO STREAMING

ONVIF compliant	H.264/H.265, M JPEG

HOUSING

Size	6.9 x 6.5 x 2 in / 175 x 165 x 51 mm
Fixed mounting	3-axis (aim precision) lock in place, low profile, solid mount, and sun shield
Color	Matte black
Weight	3.5 lbs

ENVIRONMENTAL

Environmental protection	IP67 / NEMA4 compliant
Operational temperature	-40°F to 140°F (-40°C to 65°C)
Connector	IP67 rated

ELECTRICAL

Power consumption	12.95W nominal
Input voltage	POE (IEEE802.3 af PD)

CABLE MANAGEMENT

Cable length	Up to 328 ft (100 m)
Type	Cat6 STP 22-24 AWG
Connector	10 pin circular- all-weather, impact resistant

CAMERA ACCESSORIES

Part #	VS-UNI-POLE-MNT
Description	Single Fixed Camera Mount/Bracket

VLP COMMUNICATIONS BOX

The VLP Communications Box combines processing and power in a durable, ruggedized enclosure that is equipped with an all-in-one built-in processor with GPS and PoE for up to four cameras.



SYSTEM	
CPU	Intel Gen8 Core i7-8700T (12M Cache 2.4GHz up to 4.0GHz)
Memory	2 x 8GB DDR4 2400 MHz SO-DIMM
LAN Chipset	9 x Intel i210-AT and 1 x i219 (iAMT9.5 w/ i5, i7 only) Gb/s Ethernet Controllers Onboard Support PXE and WOL

I/O	
Serial Port	3 x RS 232/422/485 (Auto Direction Control)
USB Port	4 x USB 3.0 Ports
LAN	10 x RJ45 Ports for GbE (Optional for M12 connector and 8 x PoE total Max. 120W)
Video Port	3 x DP Ports
Wi-Fi Adapter	802.11n/g/b
4G LTE / GPS	Sierra Wireless EM7511-Dual Sim Support

POWER REQUIREMENT	
Power Input	120V AC
Power Protection	Automatic Recovery - Short Circuit Protection
Power Management	Remote/Ignition connection to toggle power
Power Off Control	Power off Delay Time Setting by BIOS and Software

SOFTWARE	
Operating System	Ubuntu 18.04 64bit

GRAPHICS	
Graphics	Intel® UHD Graphics 630
Resolution	Max Resolution (DP) : 4096x2304@60Hz

STORAGE	
Type	2 x 2.5" Drive Bay for SATA Type HDD/SSD RAID 0, 1, 5 1 x mSATA

ENVIRONMENTAL	
Operating Temp.	-40°C ~ 70°C, ambient w/ 0.6m/s airflow
Storage Temp.	-40°C ~ 80°C
Relative Humidity	10% RH – 90% RH (non-condensing)
Vibration (random)	EC60068-2-64, random, 2.5G@5~500Hz, 1hr/axis with SSD
Vibration Operating	MIL-STD-810G, Method 514.6, Procedure 1, Category 4
Shock	Operating: MIL-STD-810G, Method 516.6, Procedure 1, Trucks and semi-trailers=15G (11ms) with SSD
Certifications	CE, FCC Class A, E13

MECHANICAL	
Construction	Polycarbonate
Mounting	Wall or pole mount
Weight	34.5 lbs (15,649g)
Dimensions	356(L) x 305(W) x 178(D) mm



For more information,
visit motorolasolutions.com/contactus

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved. 02-2021

1255

Fixed LPR Camera System Installation Guide

MARCH 2021

© 2021 Motorola Solutions, Inc. All rights reserved

MN007807A01
MN007807A01-AA

Legal and Support

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

© 2021 Motorola Solutions, Inc. All Rights Reserved

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

Open Source Content

This product contains Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive



The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Contact Us

For inquiries, see https://www.motorolasolutions.com/en_us/support.html **> License Plate Recognition (Vigilant)** or contact our 24 hours support staff at:

- Tel: 925-398-2079
- Fax: 925-398-2113
- Email: vigilantsupport@motorolasolutions.com

Document History

Version	Description	Date
MN007807A01-AA	Initial Release	March 2021

Read Me First

Notations Used in This Manual

Throughout the text in this publication, you notice the use of **Warning**, **Caution**, and **Notice**. These notations are used to emphasize that safety hazards exist, and the care that must be taken or observed.

WARNING: An operational procedure, practice, or condition, and so on, which may result in injury or death if not carefully observed.

CAUTION: An operational procedure, practice, or condition, and so on, which may result in damage to the equipment if not carefully observed.

NOTICE: An operational procedure, practice, or condition, and so on, which is essential to emphasize.

Special Notations

The following special notations are used throughout the text to highlight certain information or items:

Table 1: Special Notations

Example	Description
Menu key or **Camera** button	Bold words indicate a name of a key, button, or soft menu item.
The display shows `Settings Applied`.	Typewriter words indicate the MMI strings or messages displayed.
<required ID>	The courier, bold, italic, and angle brackets indicate user input.
Setup→Settings→All Settings	Bold words with the arrow in between indicate the navigation structure in the menu items.

Related Publication

The following list contains part numbers and titles of related publications. To find and download the publications, visit https://learning.motorolasolutions.com.

Part Number	Title
MN007806A01	*Vigilant ClientPortal User Guide*
MN007783A01	*Vigilant PlateSearch User Guide*
MN007808A01	*VLP Processor Installation Guide*
MN007809A01	*TAS User Guide*

Chapter 1

Hardware Overview

This section helps you to install a L5F Fixed LPR camera system.

Third-Party Hardware Components

The third-party installers provide the hardware components for installing the camera:

- ¾ in. cable for Cat6e/data to cameras.
- ½ in. liquid tight connectors and flex conduit for 120 VAC power.
- Two Metal banding and clips.[1]
- ½ in. or ¾ in. for metal cord grip for the camera cables that taps into the pole.
- Copper cabling to pull 120 VAC power from pole, photocell, or pedestal into the communications box (lengths vary by installation type).

If no premade CAT6e cables were ordered, the contractor will need to supply outdoor or UV rated Cat6e cable and RJ-45 connectors for each camera. Premade cables are available for order in 15 ft, 30 ft, and 60 ft lengths.

Additional Tools for Installation

The following additional tools are needed to perform the installation:

- Wire cutter or box cutter
- Cable stripping tool
- Needle nose pliers
- Crimp tool for shielded RJ-45 plugs with a removable die

Common Parts List

The following common parts list example are supplied by the installer:

Table 2: Item Parts List

Item	Part Number	Supplier	Quantity
Stainless Steel Banding	S-14377	ULINE	2 per box
Stainless Steel Banding Clips	S-14378	ULINE	2 per box
UV Rated Out-door Cat6e	J362404DB	Omni	15-60 ft per camera
Cat6e Metal Cord Connector	LPCG503	Arlington	1 per camera
½ in. Flexible Conduit	LTCUA050GY	Liquidtite	2-3 ft per box

[1] Simple banding is supplied for small diameter poles but most contractors opt to use their own banding rated for large diameter traffic poles.

Item	Part Number	Supplier	Quantity
½ in. Flexible Conduit Connector	NMLT50	Arlington	1 per box
¾ in. Flexible Conduit	LTCUA075GY	Liquidtite	2-3 ft per box
¾ in. Flexible Conduit Connector	NMLT75	Arlington	1 per box
UV Tie Wraps	DTP6	Dottie	Varies
1/4-20 Machine Screws	254 002	Everbilt	2 per camera
1/4-20 Locking Nuts	571 569	Everbilt	2 per camera

Table 3: Power Parts List

Item	Part Number	Supplier	Quantity
#12 Wire White	#12 Wire White	Southwire	Varies
#12 Wire Black	#12 Wire Black	Southwire	Varies
#12 Wire Green	#12 Wire Green	Southwire	Varies
Fuse Holder	Fuse Holder	Bussman	1 per box
Fuses 10 Amp	Fuses 10 Amp	Bussman	1 per box

Chapter 2

Shielded CAT6 Termination

Figure 1: Cat6e Connector



Specifications

- Connectors: RJ45 Plugs
- Rating: Cat6A
- Compatibility: 22–24 AWG stranded STP cable or ReaperHD Camera Cable

Tools

- Wire cutter or box cutter
- Cable stripping tool
- Needle nose pliers
- Crimp tool for shielded RJ45 plugs with a removable die

Cables

Table 4: Cable Pair Colors

Color Code	W	G	O	BL	BR
Description	White	Green	Orange	Blue	Brown

Table 5: Destination TS688 8-Position jack pin/pair assignments

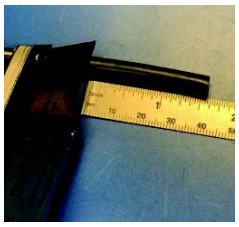
Position	1	2	3	4	5	6	7	8
Color	WO	O	W-G	BL	W-BL	G	W-BR	BR

2.1
Terminating CAT6 Cable

Procedure:

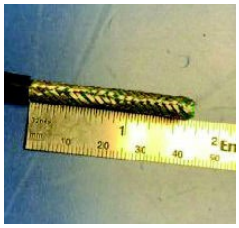
1. Slide the strain relief boot onto the cable and secure with removable tape.
2. Trim the cable jacket back about 1.5 in.

Figure 2: Trimming the Cable Jacket



3 Unbraid stranded ground wires, coil together, and move to the side.

Figure 3: Unbraiding the Stranded Ground Wires



4 Cut the center spline.

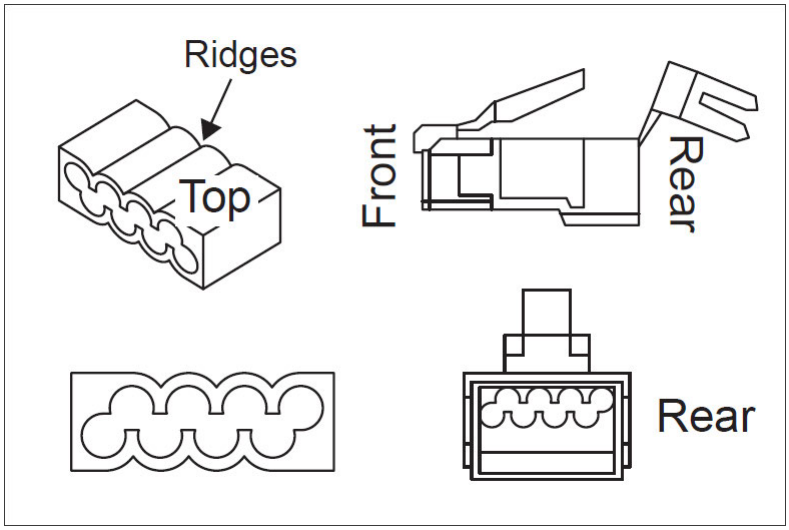
5 Trim the foil and green paper shielding.

Figure 4: Cutting the Center Spline and Trimming the Shielding



6 Orient the load bar to mate with the connector.

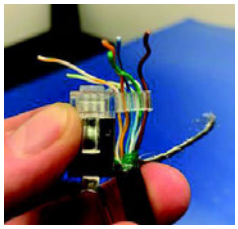
Figure 5: Orienting the Load Bar



7 Insert narrow end first and ensure that the ridges are facing up.

8 Trim the wires at an angle and gently insert the wires into the wide end.

Figure 6: Trimming the Wire



9 Trim the wires flush with the load bar.

Figure 7: Trimming the Wire Flush



10 Check if the cable jacket fits into the plug housing.

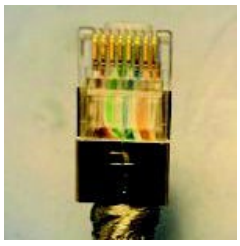
11 Insert the load bar and wires into the connector.

Figure 8: Inserting the Load Bar



12 Wrap the ground wire around the grounding collar.

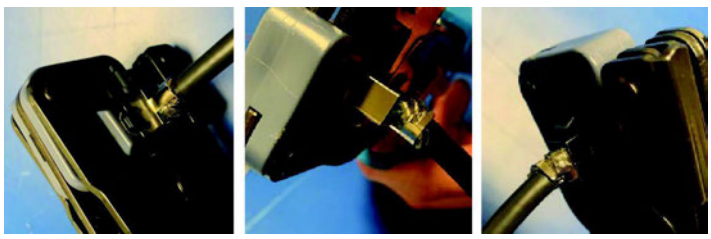
Figure 9: Wrapping the Ground Wire



13 Use a crimp tool with a removable punch die so the housing is not pierced.

14 Firmly crimp the connector.

Figure 10: Crimping the Connector



15 Visually check the wires are fully inserted.

NOTICE: For the wire color codes descriptions, see Table 5: Destination TS688 8-Position jack pin/pair assignments on page 7.

Figure 11: Fully Inserted Wires



16 Verify the ground collar is wrapped around the cable with pliers.

17 Pull the strain relief boot over the connector.

Figure 12: Pulling the Strain Relief Boot



Chapter 3

Hardware Assembly

This section helps you to perform the hardware assembly for the L5F Fixed LPR Camera System.

3.1 Camera Bracket

Figure 13: Dual-Pole Bracket

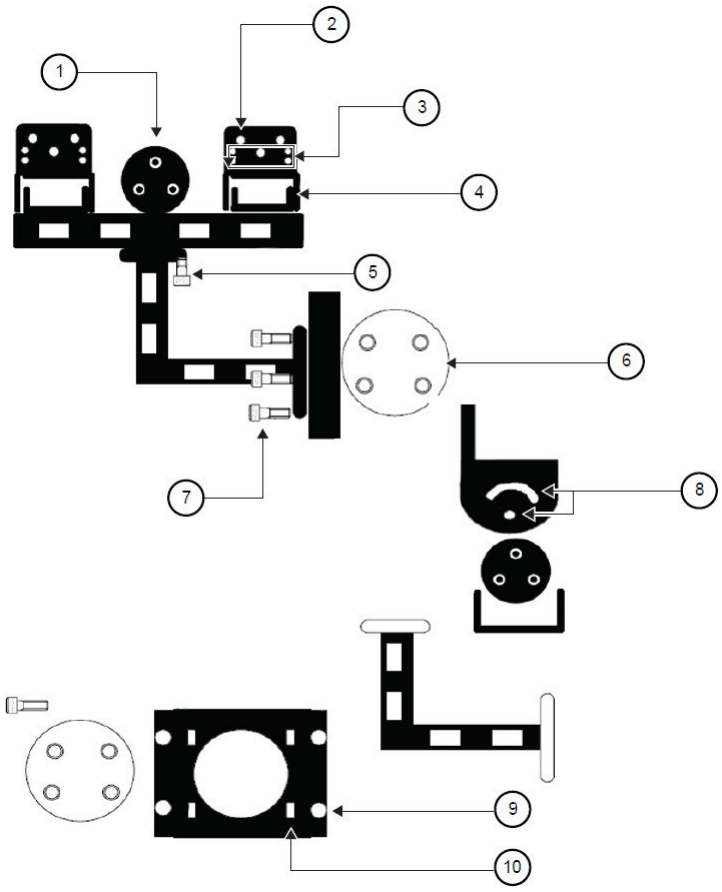


Table 6: Dual-Pole Bracket Parts Description

Parts	Description	Quantity
1	10-32 Hexagon Socket Head Cap Screws	3
2	M6-10 Button Socket Head Cap Screws.	3

Parts	Description	Quantity
3	R3 Camera Holes. Only used when mounting an R3 Camera.	n/a
4	10-32 Button Socket Head Cap Screws	8
5	10-32 Hexagon Socket Head Cap Screws. Use to mount rotating “U” shaped bracket	3
6	Round Aluminum Plate	n/a
7	5/16 in. Hexagon Socket Head Cap Screws	4
8	10/32 in. Button Socket Head Screw Caps	8 (for two cameras)
9	Use when mounting to a flat surface.	n/a
10	Use when mounting to poles; use straps provided according to pole dimensions.	n/a

3.1.1
Assembling Camera Bracket

Procedure:

1. To mount the camera to the bracket, screw down the three button socket head cap screws for each side.
2. Screw down the round bracket with three hexagon socket head cap screws.
3. To mount the bracket to the pole, use the round aluminum plate with the flat side against back of pole or wall mounting plate.
4. Screw down all all four hexagon socket head cap screws in position.
5. To mount the pole or wall mounting plate, perform one of the following actions:

Option	Actions
Mounting the plate to a wall.	Use the round screw hole.
Mounting the plate to a pole.	Use the rectangle screw hole.

Figure 14: Pole/Wall Mounting Plate

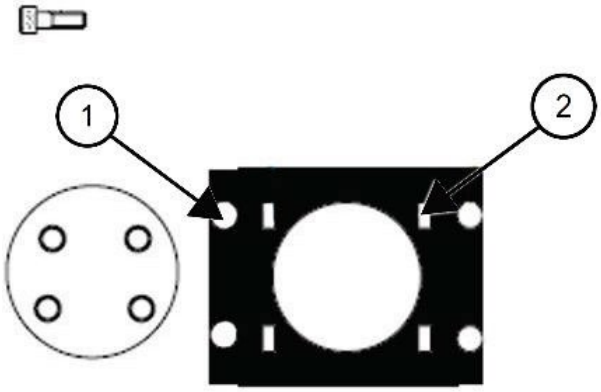


Table 7: Pole/Wall Mounting Plate Description

Number	Description
1	Round hole for wall mounting
2	Square hole for pole mounting

3.2 Uni-Pole Mount Assembly

This section describes the assembly process of mounting the camera to a uni-pole mounting kit.

The Uni-pole Mounting Kit (UNI-POLE-MNT REV.D) includes the the following mounting hardware:

Table 8: Uni-Pole Mounting Kit Parts

Parts	Quantity
¼ in. 20 Hex Screw	2
¼ in. 20 Self-clinching Nut	2
5/16 in. Hex Screw	2
5/16 in. Self-clinching Nut	2
6 in. Pole Strap	2
12 in. Pole Strap	2
Pole Bracket Base Plate	1
Mounting Arm	1
Knurl Ball	1

3.2.1
Mounting to a Vertical Pole



Procedure:

1. Use two 1/4 in.-20 Hex Screws to attach the Knurl Ball to the Mounting Arm.
2. Secure the 1/4 in.-20 Hex Screws with two 1/4 in.-20 Self-clinching Nuts.
3. Orient the Mounting Arm with the Knurl Ball facing up and the Pole Bracket Base Plate with the slots oriented horizontally as shown in the image.
4. Use two 5/16 in. Hex Screws to attach the Mounting Arm to the Pole Bracket Base Plate.
5. Secure the 5/16 in. Hex Screws with two 5/16 in. Self-clinching Nuts.
6. Slide two Pole Straps through the slots in the Pole Bracket Base Plate. The two shorter Pole Straps fit up to a 6 in. circumference pole. The longer Pole Straps fit up to a 12 in. circumference pole.

NOTICE: Make sure that the tightening screw on each Pole Strap is facing out.

3.2.2
Mounting to a Horizontal Pole

Figure 15: Mounting to a Horizontal Pole



Procedure:

1. Use two 1/4 in.-20 Hex Screws to attach the Knurl Ball to the Mounting Arm.

2 Secure the 1/4 in.-20 Hex Screws with two 1/4 in.-20 Self-clinching Nuts.

3 Orient the Mounting Arm with the Knurl Ball facing up and the Pole Bracket Base Plate with the slots oriented vertically as shown in the image.

4 Use two 5/16 in. Hex Screws to attach the Mounting Arm to the Pole Bracket Base Plate.

5 Secure the 5/16 in. Hex Screws with two 5/16 in. Self-clinching Nuts.

6 Slide two Pole Straps through the slots in the Pole Bracket Base Plate. The two shorter Pole Straps fit up to a 6 in. circumference pole. The longer Pole Straps fit up to a 12 in. circumference pole.

NOTICE: Make sure that the tightening screw on each Pole Strap is facing out.

3.2.3
Mounting to a Wall or Flat Surface

Figure 16: Mounting to a Wall or Flat Surface



Procedure:

1 Use two 1/4 in.-20 Hex Screws to attach the Knurl Ball to the Mounting Arm.

2 Secure the 1/4 in.-20 Hex Screws with the two 1/4 in.-20 Self-clinching Nuts.

NOTICE: Screws for attaching the Mounting Arm to a wall or other flat surface are not provided. The installer must determine the appropriate fasteners for the surface that the Mounting Arm is being attached to.

3.2.4
Mounting to a Pole without the Mounting Arm

Figure 17: Mounting to a Pole without the Mounting Arm



Procedure:

1. Use the two 1/4 in.-20 Hex Screws to attach the Knurl Ball to the Pole Bracket Base Plate.
2. Secure the 1/4 in.-20 Hex Screws with the two 1/4 in.-20 Self-clinching Nuts.
3. Slide two Pole Straps through the slots in the Pole Bracket Base Plate. The two shorter Pole Straps fit up to a 6 in. circumference pole. The longer Pole Straps fit up to a 12 in. circumference pole.

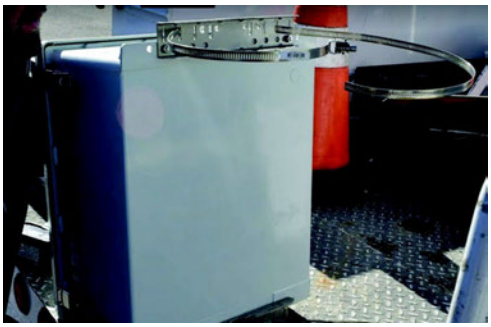
NOTICE: Make sure that the tightening screw on each Pole Strap is facing out.

3.3
Installing VLP Communications Box

Procedure:

1. To set up the VLP Communications box, place straps through the top and bottom bracket.

   Figure 18: Strapping the VLP Communications Box



2. Once straps are run through the top and bottom bracket, raise the box to your preferred height.
3. Wrap both straps around the pole.

Figure 19: Wrapping the Strap



4 Once the desired configuration of the VLP Communications box is achieved, tighten both straps to secure the VLP Communications box.

Figure 20: Securing the VLP Communications Box



5 Once the straps are fully secured, route the power and camera cable connections into the box using conduit.

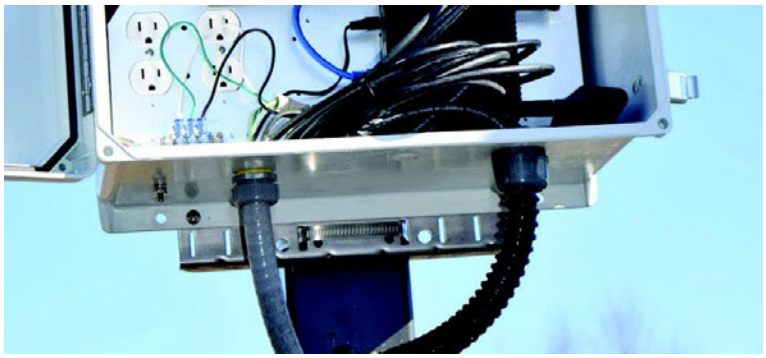
Figure 21: Routing the Power and Camera Cables



6 Use ½ in. liquid tight connectors and flex conduit for the incoming 120 VAC power connection.

7 Use ¾ in. liquid tight connectors and flex conduit for the incoming CAT6 L5F camera cables.

Figure 22: Installing the Liquid Tight Connectors



8 After the power has been connected to the box, the VLP Processor will startup.

9 Once the VLP Processor has fully booted, the L5F Fixed LPR Cameras will power up and start normal operation within 1–2 minutes.

10 Verify that each camera is operating by connecting UbuntuHD Control tool to the VLP Processor using a Windows computer.

Figure 23: Connecting UbuntuHD Control tool to the VLP Processor



11 Use UbuntuHD Control tool to configure the system for Vigilant PlateSearch. See Configuring System Using UbuntuHD Control on page 35.

Chapter 4

Software Installation

Windows Operating System Overview

For Windows Operating System, Vigilant CarDetector Fixed (Vigilant CDF) is installed as a client application with GUI that shows live video of connected cameras and lists accumulated plate detections with vehicle images. The Vigilant CarDetector Fixed application on Windows allows Target Alert Service (TAS) to connect directly to the VLP Processor inside the VLP Communications Box for expedited alerting on plates of interest (hits or plates on a hot list). The GUI can be monitored using remote desktop or using a display monitor, however it will also run unattended depending on user preference. A connection file created then exported from Vigilant PlateSearch (cloud, backend server), will need to be saved to the Vigilant CarDetector Fixed file directory

Linux Operating System Overview

The OCR application and Linux OS run on the VLP Processor inside the VLP Communnications Box. Cameras connect to the VLP Processor as it operates headless with no monitoring required or GUI available. The VLP Processor running Linux can be configured and diagnosed using an external windows PC with UbuntuHD Control tool (MiniCC) installed. MiniCC allows you to enter Vigilant PlateSearch credentials, change network scheme (ips, subnet, gateway, DNS), and view live video for aiming.

4.1
Vigilant CarDetector Fixed Configuration

4.1.1
Installing the Application

Procedure:

1. Download the latest Vigilant CarDetector Fixed (CDF) installer at http://downloads.vigilantsolutions.com/Software/CDFS_Release.zip.
2. Right-click the setup.exe icon and select **Run as administrator**.

   Figure 24: Running the CDF Installer



3. Accept the license agreement.
4. Follow the prompts onscreen to select primary OCR region and optional GPS device settings.
5. Exit installer when prompted and find the application shortcut on your desktop.

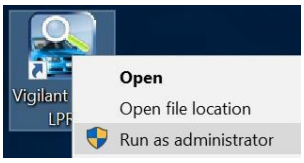
4.1.2
Configuring the Application

Procedure:

1. Right-click the application shortcut on your desktop.

2 Click **Run as administrator**.

Figure 25: Run the CDF Software



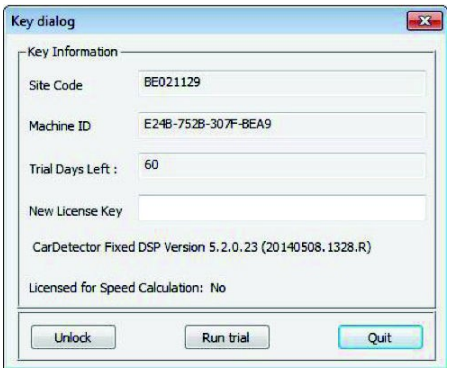
You will be prompted to enter a license key.

3 If you have not yet received the license for this system, click **Run trial**.

NOTICE: The trial installation will function for 60 days before requiring a license key.

4 If a machine has previously been licensed or already used up its trial license, this option will be disabled and a new license key will be required to proceed.

Figure 26: Key Dialog

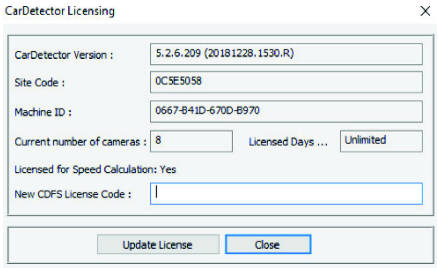


5 To request a new license key, fill out the form at: https://www.motorolasolutions.com/en_us/support/vigilant-license-key-request.html.

6 To enter the key, perform one of the following actions:

Option	Actions
Inserting the key during installation,	click **Unlock** in the dialog box to enter the key.
Inserting the key after installing and configuring Vigilant CarDetector Fixed,	**a** From the Help menu, click **CarDetector Licensing**. **b** Enter the new license key and click **Update License**.

Figure 27: CDF Licensing



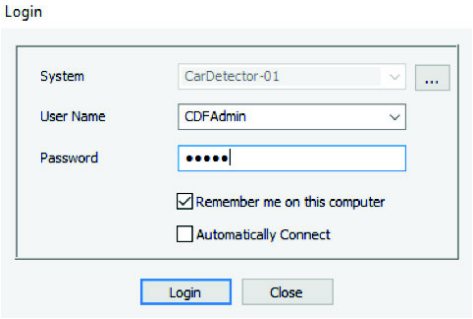
4.1.3

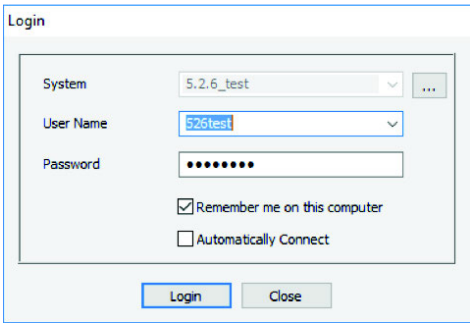
Logging Into the Application

Prerequisites: You can log into the application with or without connecting it to Vigilant PlateSearch.

Procedure:

1 Perform one of the following actions:

Option	Actions
Log in without a Vigilant PlateSearch connection,	**a** Select one of the two default usernames (CDFAdmin or CDFOperator) from the dropdown menu. **b** Enter the password and click **Login**. **NOTICE:** The default password for both logins is `12345`. **c** Select the **Automatically Connect** check box to avoid having to confirm these credentials on future logins. **Figure 28: Logging In to CDF Without Vigilant PlateSearch Connection**  **NOTICE:** When used without a Vigilant PlateSearch connection, Vigilant CarDetector Fixed will not upload your data to another server or synchronize hot list data automatically.
Log in with a Vigilant PlateSearch connection,	**a** Install your system connection file in this directory: `C:\Program Files (x86)\Vigilant Solutions\Vigilant CarDetector Fixed`. **b** Relaunch the application. **c** Select your username from the dropdown menu and log in using the Vigilant PlateSearch password. **d** Select the **Automatically Connect** check box to avoid having to confirm these credentials on future logins.

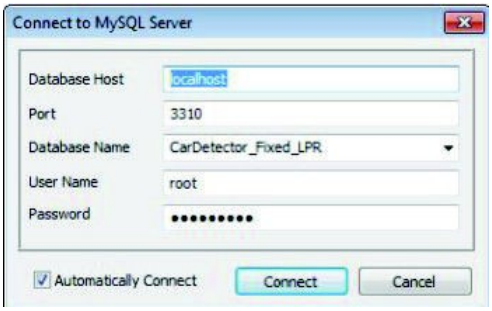
Option	Actions
	Figure 29: Logging In to CDF with Vigilant PlateSearch Connection 

4.1.4
Connecting to Database

Procedure:

1 In the **Connect to MySQL Server** window, connect the CDF software to a MySQL database.

Figure 30: Connect to MySQL Server



2 Perform one of the following actions:

Option	Actions
For new installation,	**a** Leave all default values in place except the database name that can be changed if desired. **b** Click **Connect**, then click **Yes** when prompted.
For existing system connection,	**a** Verify that the connection is live by clicking **System Configuration**. **Figure 31: Verify System Configuration** 

Figure 32: LEARN Connection



3 To verify your Vigilant Platesearch connection is active, click **Test Connection**.

4.1.5
Configuring TAS

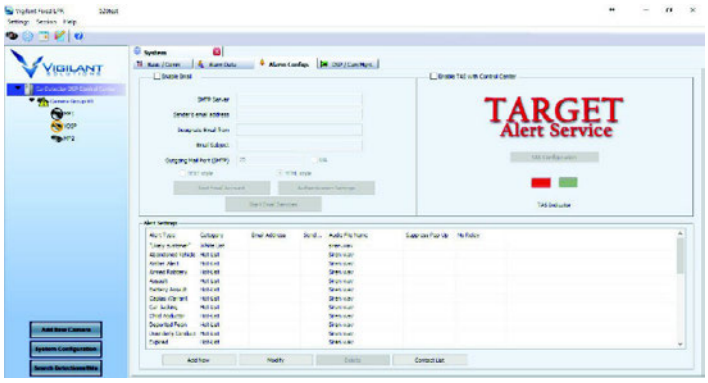
Procedure:

1 To configure TAS, click **System Configuration** and click on the **Alarm Configs** tab.

2 Select the **Enable TAS Control Center** check box.

3 Click **TAS Configuration**.

Figure 33: TAS Configuration

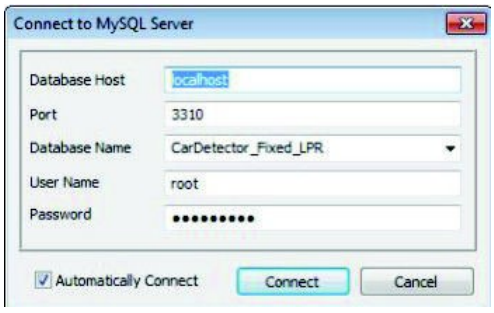


4 You will be prompted to create or connect to the TAS database.

5 If this is a new installation, leave all default values in place except database name which can be changed if desired.

6 Click **Connect**, then click **Yes** when prompted to create the new database.

Figure 34: Connect to MySQL Server



The TAS Configuration window will open.

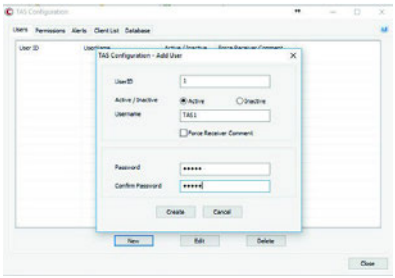
7 On the Users tab, click **New** at the bottom left to add a TAS user.

8 UserID will start at one and increment for each user you add.

9 Enter the desired TAS username and password in the labeled blanks and click **Create** to add the user.

10 The user can now connect to this CDF server using TAS client.

Figure 35: TAS Configuration-Add New User



4.1.6 Adding Cameras

Procedure:

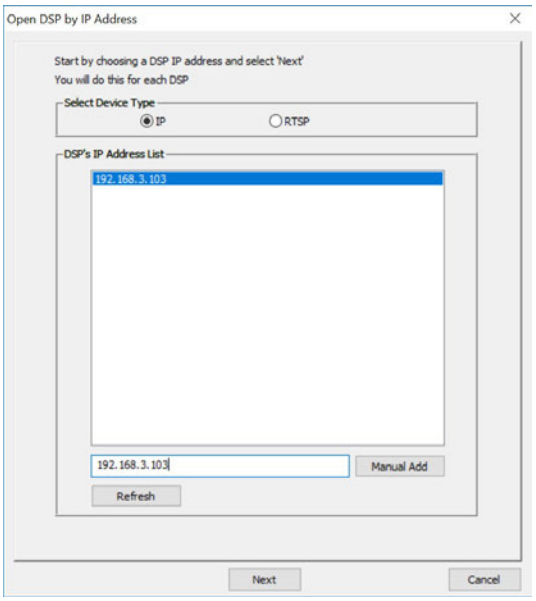
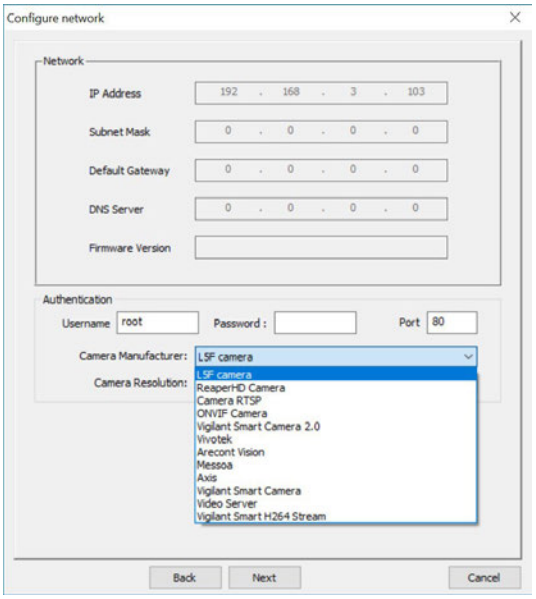
1 To add the first camera, click **Add New Camera**.

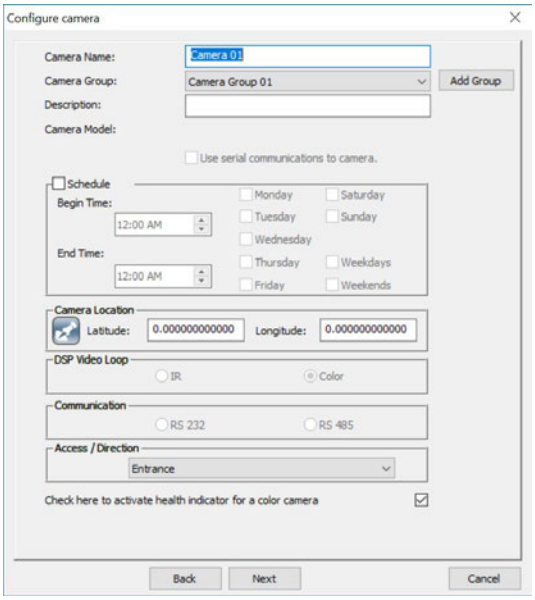
Figure 36: Add New Camera

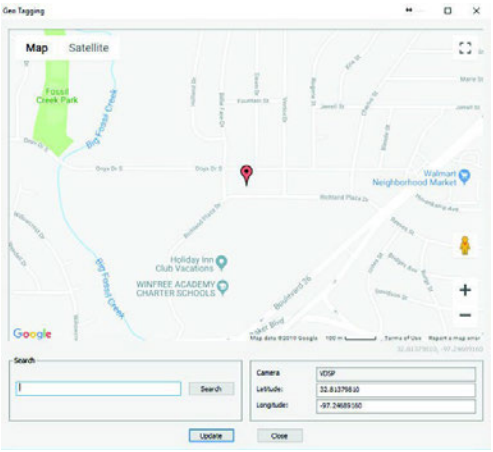
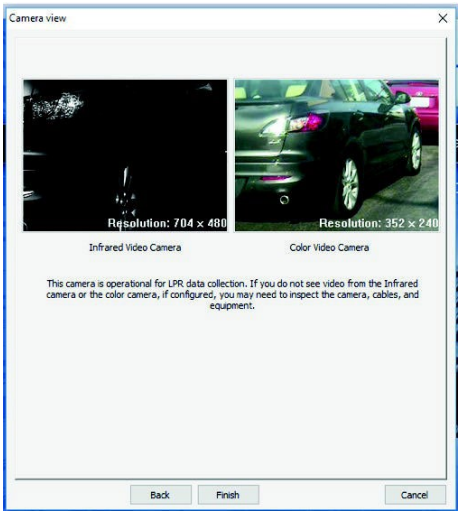


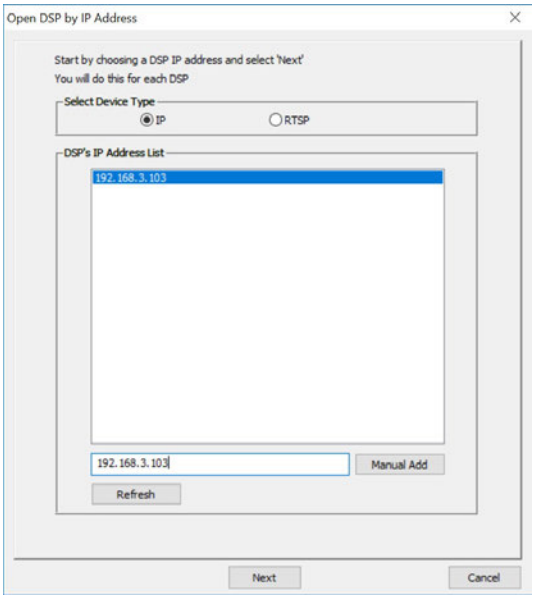
2 Depending on the type of camera that you want to add, perform one of the following actions:

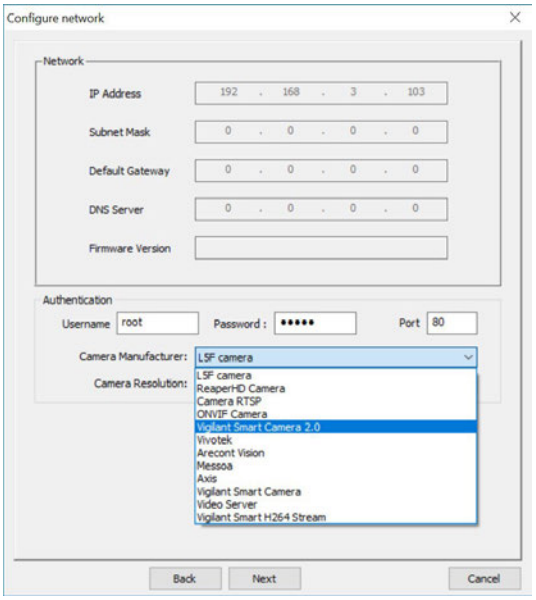
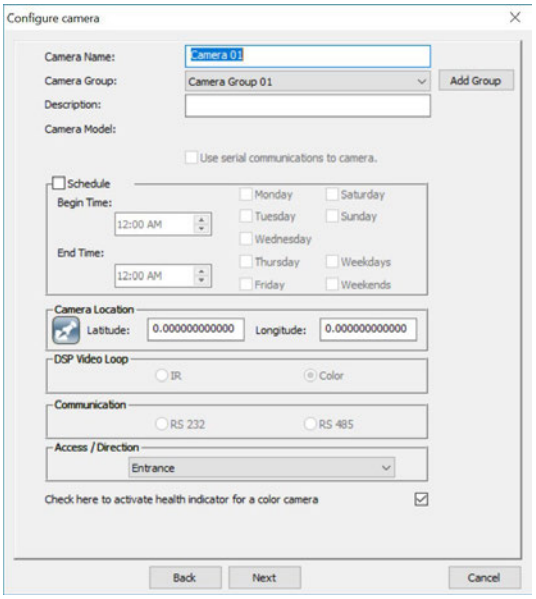
Option	Actions
Using L5F Cameras	**a** Select the **L5F** radio button. The IP addresses of all L5F cameras on the network appears in the box. **b** Select the desired camera and click **Next**. **c** If you do not see it in the list, enter the IP address of the L5F camera and click **Manual Add**. **d** Select the camera in the list and click **Next**.

Option	Actions
	Figure 37: Add L5F Camera  **e** Confirm that the boxes are populated and click **Next**. **f** If the boxes are not populated, double-check your IP address for the camera. **g** Connect to the camera from MiniCC and verify it is functioning and responding properly before continuing. **Figure 38: Configure Network**  **h** In the **Configure Camera** window, edit the text boxes as desired to configure Camera Name and Description.

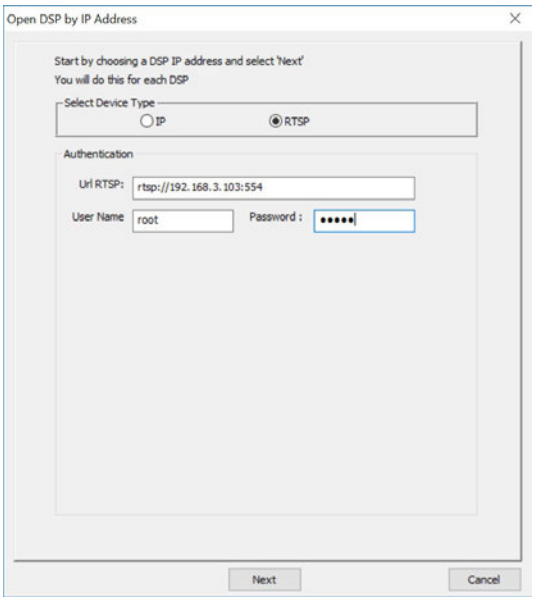
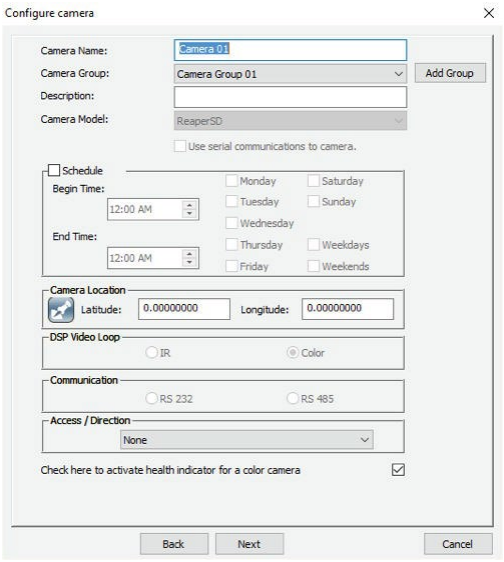
Option	Actions
	i You can create camera groups to organize your cameras on a multicamera system. **j** If you want the camera to only operate at specific times, use the **Schedule** feature to configure those times. **Figure 39: Configure Cameras**  **k** Click the pin icon under Camera Location to open the GPS search screen. **l** To set GPS coordinates, type the nearest address to the camera in the Search box at the bottom left and click **Search**. **m** Results will be shown on the left side of the map. **n** Click the address you want to use, and the map will update to show the location selected. Adjust the position of the pin as necessary to mark the camera's location precisely. **o** Click **Update**, then click **Close** to save the coordinates you've selected.

Option	Actions
	Figure 40: Geo Mapping  **p** When you're done with name, schedule, and GPS setup, click **Next**. **q** Confirm that the camera is sending video to the CarDetector software. **r** In the Camera view window, you will see live video streams from both the IR and color overview cameras of the L5F. **s** Verify that both streams are live and click **Finish**. **Figure 41: Camera View**  **CAUTION:** The software will immediately update the firmware version on the L5F camera if an update is available. Do not interrupt or disconnect either device during the firmware update process. Doing so may seriously damage your L5F camera.

Option	Actions
Using Third-Party Camera	**a** To add the camera, select the **IP** radio button. **b** Enter the IP address of the Third-Party Camera and click **Manual Add**. If the device is on the network, it will appear in the box above. **c** Select the IP address in the box and click **Next**. **Figure 42: Third-Party Camera IP Address**  **d** Confirm that the Network boxes are populated. **e** Enter the camera's username, password, and http port (80 by default) in the provided boxes. **f** Select **Vigilant Smart Camera 2.0** from the dropdown menu and click **Next**.

Option	Actions
	Figure 43: Third-Party Camera Configure Network  **g** If the **Next** button is unavailable, the software cannot ping the camera. Try connecting to it in Internet Explorer to verify it's online and check your credentials. **h** Fill in camera name, schedule (optional), GPS coordinates, and access/direction (optional). **i** Click **Next**. **Figure 44: Third-Party Camera Configure Camera** 

Option	Actions
	j Confirm that the camera is sending video to the Vigilant CarDetector software. **k** Verify that the video stream in the window is live, then click **Finish**. **Figure 45: Third-Party Camera View**  **l** If the stream does not appear, verify you can connect to the camera and view the stream with Internet Explorer. **m** You will still need to configure your Third-Party Camera to optimize it for LPR performance (see separate documentation).
Using RTSP	**a** To add an RTSP camera, select the **RTSP** radio button. **b** Enter the RTSP URL of the camera. This is normally "rtsp://" followed by the IP address of the camera. **c** Enter the Username and Password of the camera. This information is normally included in the camera documentation. **d** When the information has been entered, click **Next**.

Option	Actions
	Figure 46: RTSP IP Address  **e** Fill in camera name, schedule (optional), GPS coordinates, and access/direction (optional) and click **Next**. **Figure 47: RTSP Configure Camera**  **f** Confirm that the camera is sending video to the LPR software. **g** Verify that the video stream in the window isinive, then click **Finish**. **h** If the stream does not appear, verify you can connect to the camera and view the stream with Internet Explorer.

Option	Actions
	Figure 48: RTSP Camera View 

3 Repeat step step 2 to add all of your cameras to the software.

4.2 Vigilant PlateSearch Camera Configuration

4.2.1 Checking Operating System

Procedure:

1 Check your purchase order documents.

If Vigilant CarDetector Fixed software is listed in the product description, the Operating System (OS) on the VLP is Windows.

2 Connect a monitor and keyboard.

For Windows OS, a blue login screen appears.

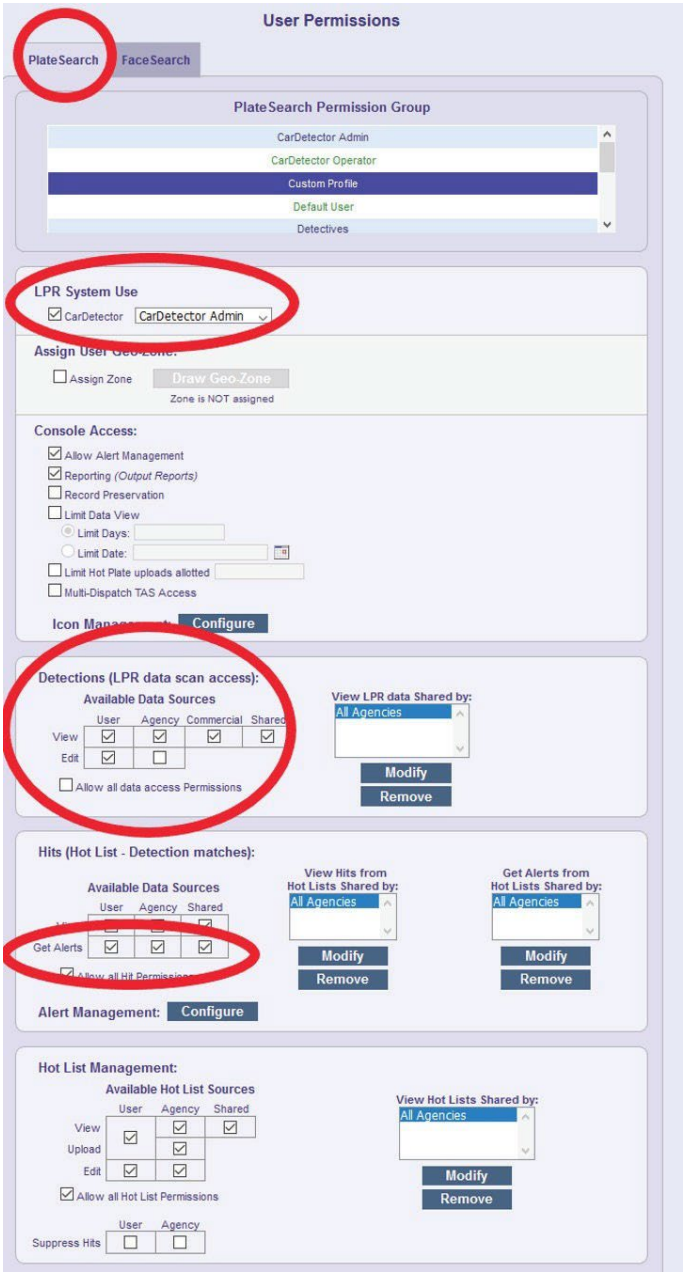
For Linux OS, a black command line, terminal screen appears.

4.2.2 Creating a User

Procedure:

1 As an agency manager, go to **PlateSearch→User Management**.
2 Click **Add New User** or **Search/Modify Users** if the user already exists.
3 Ensure that the LPR System use is selected with **CarDetector Admin** in the dropdown menu.
4 To use this account to check data, enable the detection viewing settings.
5 To enable the user to generate alerts, turn on the alerting settings.
6 Click **Create**.

Figure 49: User Permissions



For Windows Operating System (OS), you will use the created user when logging into Vigilant CDF. If you have placed your connection file correctly, you should see the user as available choice from the login dropdown menu when starting Vigilant CDF.

For Linux OS, save the name of the created user as you will need to enter it into the VL Processor using UbuntuHD Control later.

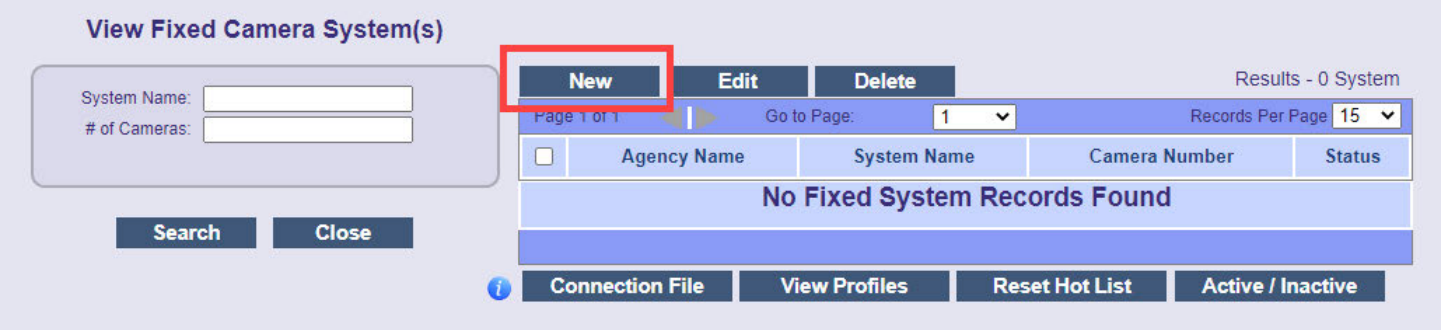
4.2.3
Creating a System

Prerequisites: This section is only applicable for the Agency Managers. To create a fixed system, ensure that the agency is already created in Vigilant Platesearch.

Procedure:

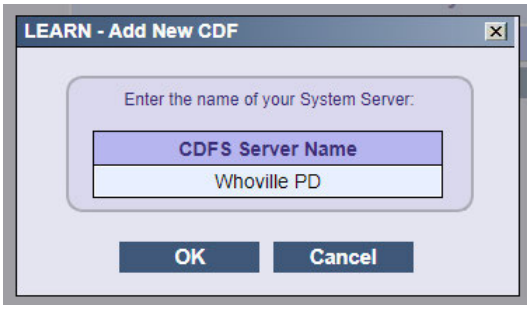
1 Go to **PlateSearch→Agency Management→Fixed Camera System→New**.

Figure 50: Create New Fixed System



2 Name the camera site appropriately.

Figure 51: New Fixed System Name



3 Set the OCR Region.

Figure 52: OCR Region

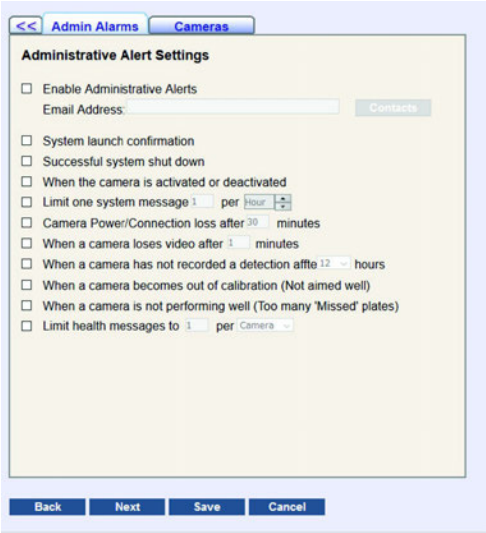


4 Based on the operating system that you are using, perform one of the following actions:

- For Windows OS, continue to step 5.
- For Linux OS, save the name of the system that you just created as you need to enter the system name into the VLP using UbuntuHD Control tool.

5 Click the **Admin Alarms** tab and ensure that the system is set up properly.

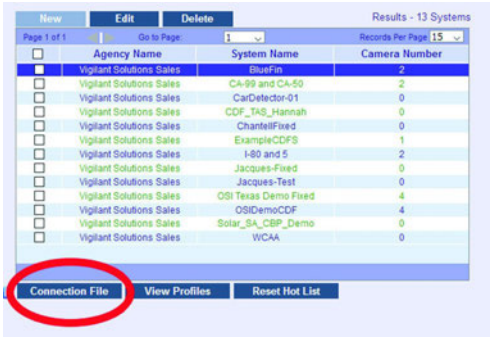
Figure 53: Admin Alarms



6 Click **Save**.

7 Download your connection file by highlighting your system and clicking **Connection File**.

Figure 54: Connection File



8 Save the connection file and transfer it to the VLP Processor inside the VLP Communications Box.

9 Place the file in the Root Directory of the Vigilant CarDetector Fixed Program: `C:\Program Files (x86)\Vigilant Solutions\Fixed LPR`.

4.2.3.1
Configuring System Using UbuntuHD Control

Procedure:

1 To configure the VLP Processor's connection to Vigilant LEARN, click **LEARN**.

2 Enter the username and password of the user created in Vigilant LEARN.

3 Enter your Agency name

4 Enter the System name.

5 Enter the Longitude and Latitude GPS coordinates by clicking the **Location** symbol.

6 Leave the other text boxes at the default values they have.

7 Click **Apply**, then click **Test Connect**.

- If you get a success message, proceed to step step 8.
- If you get `Operation failed: Invalid Username/Password`, check the username and password.
- If you get `Operation failed: Unknown error`, go back to **Change IP** button and check the network configuration for ***<enp3s0>*** (IP, Subnet, Gateway, and DNS).

8 Close the **LEARN** window when complete.

9 To name each of the camera, click **Change Source Type**.

10 Check the box next to **Enable**.

11 Enter the camera IP in the **Address** box.

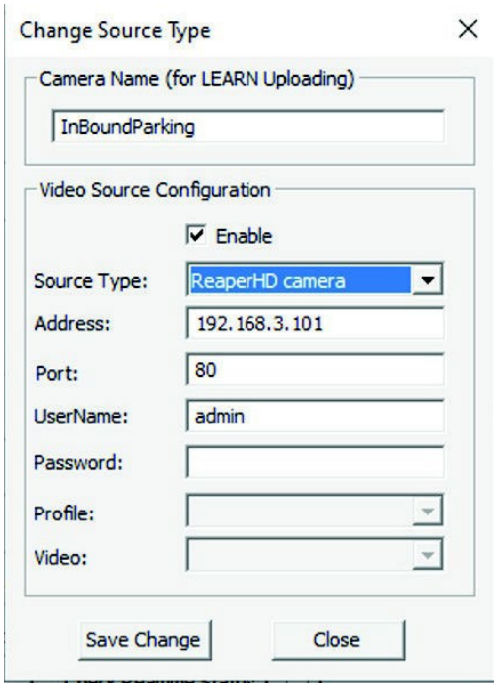
NOTICE: By default, the IP addresses for cameras are 192.168.3.100-103.

12 Enter a Camera Name (for Vigilant LEARN Uploading) that uniquely identifies this camera.

13 Use **Port** of `80`.

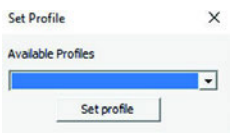
14 Leave the **UserName** as ***<admin>*** and leave the **Password** blank.

Figure 55: Configuring Source Type



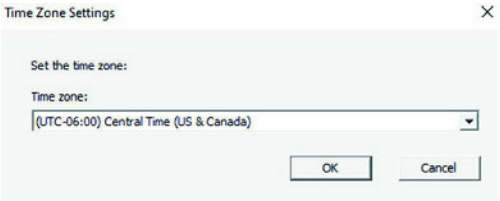
15 To set the OCR profile, click **Set Profile** and select the correct state OCR profile.

Figure 56: Set Profile



16 To set the Time Zone, click **Set the time zone** and select the correct GMT.

Figure 57: Time Zone Setting



17 To set the Network Configuration, click **Change IP**.

a Select **enp3s0→Static**.

b Change the IP, Subnet, Gateway, and DNS to work with your router and network settings.

c Check **DHC** then click **Write to Broad**.

d The system will save settings and do a soft reboot. Wait for 60 seconds.

18 To check your configuration settings, click **Get Health Information**.

Verify that the following parameters are correct:

- **IP Configuration** shows the correct settings for your router.
- **Engine Profile** is the correct state profile you selected.
- **LEARN Account Information** shows the correct credentials.
- **Current Time** is accurate.
- **GPS Coordinates** is showing the correct values.
- Check **Scans Upload status**, **Total Scans Upload**, and **Total Plate in Vigilant PlateSearch queue** for the number of plates that you have scanned that should be sent to LEARN.

4.2.4 Verifying the System Connection

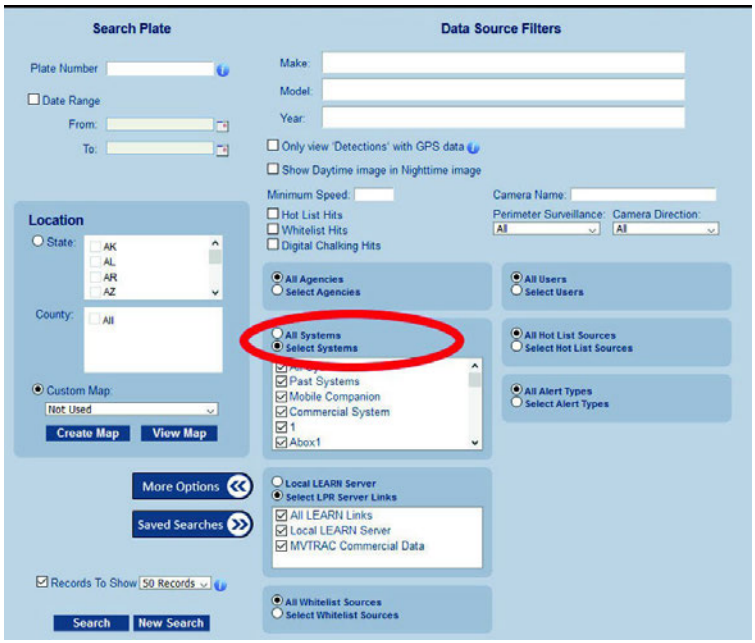
Prerequisites: Log in to Vigilant Platesearch using the credentials you just created.

Procedure:

1 Go to **PlateSearch→License Plate Query→More Options**.

2 Filter by the system you just created.

Figure 58: Verify System Connection



Returns generated will be plate detections from only this system.

If the system connection is created successfully, you are able to view the following results:

- Able to view the plate detections from the system.
- Vigilant CarDetector Fixed is connected.
- The detections are sent to the Vigilant Platesearch cloud server.

NOTICE: If the system connection is not created successfully, contact Vigilant Support.

L5Q

QUICK DEPLOY LICENSE PLATE RECOGNITION CAMERA SYSTEM

LICENSE PLATE RECOGNITION WITHIN REACH LIKE NEVER BEFORE

Build or expand an existing camera network with this affordable, easy-to-deploy-anywhere license plate camera system. This complete, quick deploy solution, paired with either Vigilant PlateSearch or Vigilant ClientPortal empowers you to receive real-time alerts, conduct comprehensive searches as well as leverage advanced analytics to uncover new insights and operate more efficiently.



KEY FEATURES

- Flexible power options - AC/DC or solar
- Built-in cellular communications
- Redeployable, all-in-one system design
- Rugged construction - IP66 rated
- Simple hot/shielded list management
- Robust, real-time alerting options
- Comprehensive search and reporting
- Configurable data retention settings
- Advanced vehicle location analytics
- Dedicated parking enforcement tools
- Customer-managed data access and sharing
- 3rd party LPR system integration

CAMERA SPECIFICATIONS

CAMERA PERFORMANCE	
Optimal focal length	50 ft (15 m)
Capture range	< 75 ft (23 m)

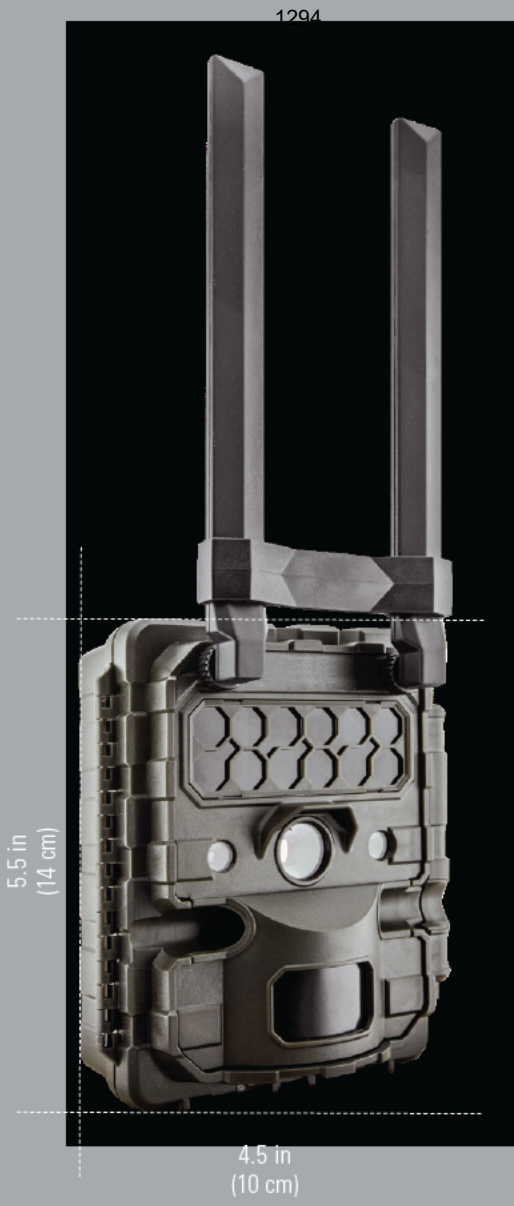
OPTICS	
Image	3 MP image sensor
Capture speed maximum	85 mph (recommended deployment speed 45 mph or less)

HOUSING	
Size	5.5"H x 4.5"W x 2.5"D (14 x 10 x 6.4 cm)
Fixed mounting	Low profile, pole mount bracket solution
Color	OD Green

ENVIRONMENTAL	
Environmental protection	IP66
Operational temperature	-20°F to 120°F (-29°C to 50°C)

CABLE MANAGEMENT	
Cable length	12 ft (4 m)
Type	Shielded power cable
Connector	Custom 12V barrel

SOLAR PANEL POWER UNIT	
Solar panel power	10W
Battery capacity	108 Wh
Product warranty	1 year
Dimensions	11.75"H x 12.0"W x 8.25"D (30 x 30.5 x 21 cm)
Included accessories	12 ft (4 m) shielded power cable



For more information, visit
www.motorolasolutions.com/l5q

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**
MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2020 Motorola Solutions, Inc. All rights reserved. 12-2020



a red violet company
(NASDAQ: RDVT)

Fusion Center Increases Investigative Efficiency with idiCORE™

Overview

A law enforcement fusion center in the Southeastern United States protects one of the largest counties in America with full scope police and investigative services. The Center is responsible for all manner of crime enforcement, ranging from property crimes to violent crimes. In order to protect its citizens, it relies heavily on identity intelligence data to provide amplifying information that can efficiently and accurately support ongoing investigations.

We spoke with leading intelligence analysts and law enforcement officers about how identity intelligence is leveraged during investigations.

Challenge

> "We needed a system that could provide us with actionable intelligence we could rely on, without fidelity concerns of the data. False positives, specifically around phone number accuracy, were causing investigations to take more time than they should."
>
> – Criminal Intelligence Analyst

Often, knowing where to start in an investigation can present the most daunting challenge for law enforcement professionals. While interviewing witnesses and reviewing video evidence are always helpful, in today's hyper-connected world getting a deep understanding of who a suspect is, where they reside and who they associate with can make the difference in quickly solving a case or allowing a potential criminal to remain free.

Identity intelligence (unique information about individuals that helps prove who they are) is widely used by law enforcement agencies to bolster normal investigative tactics and government data sources, but legacy systems often return poor data and false positives resulting in more work and longer case resolution.

The Fusion Center, not satisfied with legacy providers, sought cloud-native identity intelligence providers to augment existing capabilities in order to more accurately and quickly support investigations.

Solution

Before deciding on the IDI solution, the Center evaluated other solutions but found that the precision and recall of their data was not sufficient.

The IDI solution, idiCORE, increases analytic efficiency!

idiCORE is powered by a cloud-native platform, utilizing machine learning algorithms that increase confidence that the first record is correct, limiting the need for multiple searches or pivoting to different records.



Phone Number Matching

Phone number matching was reported to be 30% better than legacy systems, giving analysts and officers much greater confidence in corroborating facts in fast-moving environments.



Familial Relationships

Familial relationships were reported to be 40% better than legacy systems, allowing investigators to glean deep insights into a suspect's 'pattern of life' and gain a deeper understanding of dynamic operating environments prior to real-world engagement.

Results

The Center estimates that the idiCORE solution has helped them reduce time spent on phone number analysis by 30% – leading to more cases cleared and with significantly greater accuracy than prior to deployment.

The idiCORE solution also has started to change internal interaction within the Center. The Intelligence Analysts at this Fusion Center reported that because of the data accuracy of idiCORE, their credibility with detectives and other sworn officers has improved.

"The idiCORE solution is much more user friendly, faster and more accurate than our existing providers. We've come to rely on idiCORE for any investigation that entails phone numbers given how accurate the matching is within the system.

Our investigators are very confident that the first search in idiCORE will return accurate results, which provides a real improvement in our investigative efficiency."

Criminal Intelligence Analyst

"Gone are the days of bad data leading to investigators wasting time and energy chasing leads that simply didn't exist. idiCORE™ gives us confidence in our identity intelligence data, enabling us to clear more cases more quickly, resulting in a much more efficient department overall."

Control Officer, Fusion Center

"Because of how accurate the data is and how quickly we can get it into the hands of investigators, we're seeing a significant increase in requests for analytic assistance in cases. It's been a real benefit not just to officers, but to the working relationship between analysts and sworn officials."

The Section Manager of the Center

For more information about this case study or to learn more about IDI and its solutions, please contact IDI at 855.842.1410 / sales@ididata.com or sign up for a FREE Trial.

IDI is a red violet® company.
To learn more about red violet, click here.

©2021 Interactive Data, LLC. All rights reserved.
IDI and related marks are trademarks of Interactive Data, LLC.

LYNN FLOCK FIXED (ALPR) ACTIVITY

#	Report #	Date	Action - Incident	Result
1	N/A	11/13/21	Assist Providence RI, PD Homicide Investigation	On 11/15, Providence, RI PD investigators contacted LPD regarding a homicide reported there on this date. It is believed the homicide occurred on 11/13. The victim's phone was confirmed being in Lynn on this date. A check of the victim's license plate on the Flock database confirmed that the victim's vehicle passed an ALPR on 11/13. This assisted in the confirmation of the timeline on the matter and the ALPR in question was in the area of suspect's family residence.
2	21079094	11/17/21	Stolen M/V Recovery	LPD received stolen M/V alert for MA Reg. 324E10. Info. broadcast to Patrol Units of last location. Vehicle stopped at 41 Market St. – Complaint against operator Vehicle towed.
3	21079247	11/18/21	Assault with a Firearm	Subjects assaulted by male with a firearm at 124 Boston St. (2) suspects fled on motorcycles. Det. Hilton was able to ID the subjects and vehicles involved and bring charges against subject who brandished the fire.
4	N/A	12/1/21	Assist Everett PD Shooting Incident	On the evening of 12/1, there was a shooting incident at the casino in Everett. A specific vehicle was identified which had ties to Lynn. A query of the Flock ALPR system revealed that the vehicle entered Lynn via the Lynnway shortly after the shooting and exited a short time later via Boston St. into Saugus. The vehicle was later located in Saugus.
5	21082534	12/1/21	Shots Fired Incident	Shots fired in the area of 18 Alley St. Search was conducted of the ALPR cameras to try and ID suspect vehicle without success.
6	N/A	12/7/21	Wanted Subject	I created an alert for a vehicle believed to be in the possession of a subject with ties to Lynn wanted for an armed home invasion in Amesbury. The alert remains active as subject is still at large. The vehicle hit on an ALPR on 12/5/21.
7	21085558	12/14/21	Stolen M/V Recovery	LPD received stolen M/V alert for PA Reg. KKC1761. Info. broadcast to Patrol Units of last alert location. Vehicle located in parking lot nearby. Operator arrested, active narcotics user. Vehicle likely being used to commit other crimes.
8	21085936	12/15/21	Stolen M/V Recovery	LPD received stolen M/V alert for UT Reg 8NY611. Info. broadcast to Patrol Units of last alert location. Vehicle located in parking lot nearby. Vehicle was overdue rental – operator summonsed for Receiving a Stolen M/V.
9	21086903	12/19/21	Missing Person Homicide Investigation	A woman from Woburn reported missing on 12/19. She was last known to be with a male on the evening of 12/18 who was in possession of a particular vehicle that was registered at 49 Laighton St. LPD Flock ALPR's searched the database and vehicle hit on an ALPR outbound on Lynnfield St. on the evening of 12/18. Suspect l kely going to Woburn to pick up victim who was eventually found deceased and a victim of a homicide. ALPR information solidified a timeline which assisted investigation.
10	21086983	12/20/21	Shots Fired Incident	Shots fired in the area of 130 Union St. Vague description of vehicle involved provided. Search was conducted of the ALPR cameras to try and ID suspect vehicle without success.
11	21087401	12/21/21	Warrant Arrest	LPD received an alert that a subject associated with NH Reg. 4783893 had an active arrest warrant for narcotics charges from NH which they would rendite for. Information was broadcast to LPD Units and the vehicle was located and stopped at Lawton and Western Aves. The subject of the warrant was not in the vehicle, however, a male passenger had an active MA arrest warrant from Newburyport and he was arrested. Subjects involved likely in Lynn to engage in narcotics activity.
12	N/A	TBD	Hit & Run M/V	Sgt. Hunter reported that Flock ALPR used to solve a recent Hit-Run MVA. He searched the cameras for the time of the crash and vehicle hit on an ALPR minutes after the crash. He investigated and located vehicle. Spoke with owner who admitted to the crash. I will get report #, etc. from Sgt. Hunter.
13	21087444	12/22/21	Stolen M/V Recovery	LPD received stolen M/V alert for MA Reg. 1DNM444. Info. broadcast to Patrol Units of last alert location. Vehicle stopped on Spring St.

				Operator arrested for Receiving Stolen M/V. He was also found in possession of cocaine and he had multiple warrants. Vehicle likely used to traffic narcotics.

LYNN POLICE DEPARTMENT		Department Manual: Policy No. 22.1
Subject: **Automated License Plate Reader System**		
Reference: **Supersedes Policy No. 22**		
Effective Date: **August 15, 2011** **Updated:** **December 2, 2021**	**Issuing Authority** _____ **Christopher P. Reddy** **Chief of Police**	

22.1 PURPOSE

The purpose of this Policy is to establish guidelines and procedures for the proper use and application of Automated License Plate Recognition (ALPR) systems, the management of the data, and the maintenance of the equipment.

22.2 POLICY

The availability and use of (ALPR) systems have provided many opportunities for the enhancement of productivity and effectiveness, as well as increased safety to the public and law enforcement. It is the policy of the Lynn Police Department (LPD) to only utilize this technology in the furtherance of official and legitimate law enforcement operations and public safety. All members are expected to abide by the guidelines set forth herein when using an (ALPR) system.

22.3 ACRONYMS AND DEFINITIONS

22.3.1: *Alert*: A visual and/or auditory notice that is triggered when an (ALPR) system receives a potential hit on a license plate.

22.3.2 *(ALPR)*: Automated License Plate Recognition. Automated License Plate Recognition (ALPR technology uses high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The (ALPR) system captures an image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to the CJIS-NCIC Hot file database.

22.3.3 (ALPR) Operator: Trained Lynn Police Department personnel authorized to utilize (ALPR) systems and equipment.

22.3.4 (ALPR) Administrator: Designee of the Chief of Police responsible for compliance with all applicable laws and regulations pertaining to (ALPRs) as well as providing access and training to Department personnel in the operation of (ALPR) systems.

22.3.5 Alert Data: Information captured by an (ALPR) relating to a license plate that matches the license plate on a "hot list".

22.3.6 (ALPR) Data: Scan files, alert data, and any other documents or data generated by, or obtained through, utilization of an (ALPR) system.

22.3.7 (ALPR) Data Query Logs: A record of a search or query of (ALPR) data.

22.3.8 (ALPR) System: The (ALPR) camera and all associated equipment and databases operated by the Lynn Police Department. This includes fixed (ALPR) cameras that are attached to a structure, such as a pole, a traffic barrier, or a bridge, as well as mobile (ALPR) cameras that are deployed from a law enforcement vehicle or other equipment for mobile deployment.

22.3.9 (GPS): Global Positioning System.

22.3.10 "Hit": An alert that a license plate matches a record maintained in an (ALPR) database related to stolen vehicles, wanted vehicles, or other alert type files that support investigation or which have been manually registered by a user for further investigation.

22.3.11 "Hot List": License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to "hot lists" circulated among law enforcement agencies. "Hot List" information can come from a

variety of sources, including the Commonwealth of Massachusetts Department of Criminal Justice Information Services (DCJIS), the National Crime Information Center (NCIC), as well as national Amber Alerts and Department of Homeland Security watch lists. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported "hot lists", users may also manually add license plate numbers to "hot lists" in order to be alerted if and when a vehicle license plate of interest is "read" by the ALPR system in accordance with a legitimate law enforcement purpose.

22.3.12 "Hot List" Download: The method by which the "hot list" data is transferred to a computer within a law enforcement vehicle or at a fixed terminal.

22.3.13 Optical Character Recognition (OCR): The technology that supports the automated reading and digitizing of images of license plates that are captured by an (ALPR) system.

22.4 PROCEDURES

22.4.1 General: (ALPR) systems and associated equipment and databases, whether owned or under the control of the Lynn Police Department, are authorized for official use only. Misuse of this equipment and associated databases or data may be subject to sanctions and/or disciplinary actions, as determined by the rules and regulations of the Department.

22.4.2 Administrative and Technical Support

- **Administrative Support:** The (ALPR) Administrator will oversee the Department's (ALPR) operations. The Captain of the Criminal Investigation Division shall serve in this capacity.

  Assigned duties shall include:

- Ensuring that the (ALPR) system is used only for appropriate Department business and in accordance with this policy;
- Monitoring the use of the (ALPR) and schedule periodic audits;
- Recommending updates to the (ALPR) policy;
- Keeping informed of legal decisions, trends, and case law concerning (ALPRs);
- Coordinating with other Department personnel regarding the maintenance and retention of data;

- Maintaining records identifying approved (ALPR) deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to (ALPR) usage;
- Authorizing any requests for (ALPR) systems use or data access according to the policies and guidelines of this agency

Technical Support: The Sergeant assigned to the Traffic Unit shall be designated as the Program Technician. In his absence, the other Traffic Unit personnel may assist as needed. The duties of the Technician shall include:

- Training designated officers in the proper operation of (ALPR) systems;
- Documenting those trained as Operators and reporting this information to the Training Unit;
- Providing periodic equipment checks to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be removed from services until repaired;
- Assist other department personnel as needed.
- Ensuring that designated and trained personnel examine equipment on a regular basis to ensure functionality and camera alignment and removing from service any equipment that falls outside expected functionality until deficiencies have been corrected;
- Ensuring the proper selection of the personnel approved to operate the (ALPR) system and maintaining an adequate number of trained and authorized users

22.4.3 Maintenance and Retention of Data

The Record Department OIC shall be responsible for the maintenance and retention of data stored by Lynn Police Department (ALPR) systems in accordance with MA Public Records Laws.

22.4.4 (ALPR) System Usage

- (ALPR) systems and information shall be accessed and used only for official and legitimate law enforcement operations and public safety related purposes, and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

- Only users who have been designated by the (ALPR) Administrator and properly trained in the use and operational protocols of the (ALPR) system shall be permitted to use a system. Only those users with an approved login and password will be allowed access to an (ALPR) system.

- **Authorized User Alert Profile**: Personnel who have been designated as an **authorized user with an approved login and password for access to the Flock Safety ALPR System** must establish an alert profile at the time of initial login. In order to minimize disruption from excessive alerts, and to avoid alerts based on categories that are not actionable without a simple CJIS query, all personnel must comply with the following schedule for alert notifications:

    - **Authorized Categories:** The following categories for an alert profile are authorized:
        - Stolen Vehicle
        - Warrants
        - Missing Person
        - Protective Order
        - NCMEC Amber Alert
        - Missing Child
        - LPD hot list

    - **Prohibited Categories:** The following categories for an alert profile are prohibited:
        - Sex Offender
        - Stolen Plate
        - Gang Member or Suspected Terrorist
        - CPIC Data Records
        - Immigration Violator
        - Violent Person
        - Protective Interest
        - Supervised Release

Exceptions to these requirements for specific users may be authorized by the (ALPR) Administrator – the Captain of the Criminal Investigations Division. These exceptions shall only be made to further a specific investigation or other public safety purpose.

- Searches of historical (ALPR) data shall be done in accordance with established departmental policies and procedures.

- Requests to use an (ALPR) system during nontraditional deployments, i.e. special operations or criminal investigations, must be approved by the Administrator. In their absence, requests may be forwarded to a Deputy Chief or the Chief.

22.5 Operational Procedures

22.5.1 Manual Entry of Data

- Personnel may become aware of license plate numbers or vehicles of interest from a specific incident or investigation and may seek to have this information be entered into LPD (ALPR) systems. The entry of this information will trigger alerts to be forwarded to LPD personnel and other designated agencies. **This information may be entered only by an authorized Lynn Police Department supervisor and only for official and legitimate law enforcement or public safety operations.**

- For all manual license plate entries, a verification of the license plates shall be queried via CJIS to verify the plate to be entered is accurate.

- Manual entries may include, but should not be limited to, an AMBER Alert, Missing Child Alert, Missing College Student Bulletin, Be On Look Out (BOLO), Attempt To Locate (ATL), or Wanted or Missing Person broadcast or bulletin, in which a license plate number is included. Such manual entries must be manually updated when the information changes or is no longer current.

- Manual entries may also include specific descriptions of vehicles which are being sought for specific crimes or in accordance with investigations.

22.5.2 (ALPR) "Hits" and Alerts:

Prior to initiation of a stop based on a "hit" or alert:

- Users shall visually verify that the vehicle plate number matches the plate number queried by an (ALPR) system, including both alphanumeric characters of the license plate and the state of issuance.

- Users shall verify the current status of the plate through the Commonwealth's Criminal Justice Information System (CJIS), National Crime Information Center (NCIC) Department's Records Management System (RMS), or other appropriate source of data prior to a stop when circumstances allow or as soon as practicable. (Confirm the vehicle is stolen, etc.)

22.5.3 Mobile (ALPR) Procedures:

- At the start of each shift, personnel assigned to Department vehicles equipped with LPD mobile (ALPRs) shall ensure that the (ALPR) system has been updated with the most current hot lists available.

- At the beginning of each tour of duty, users should verify the aim of the (ALPR) camera(s) to ensure it is focused on the correct lanes of traffic.

- (ALPR) equipment should be cleaned and maintained according to the manufacturer's recommendations.

- Any damage to (ALPR) systems will be reported immediately according to the Department's established policy and procedures related to the loss of, or damage to, the Department's equipment.

- When not in use, (ALPR)-equipped vehicles should be secured.

22.6 INFORMATION MANAGEMENT

22.6.1 (ALPR) Data Query Records

- In accordance with agreements between the Lynn Police Department and contracted (ALPR) vendors, Department vendors will maintain a record for each transaction conducted on Department (ALPR) systems that will include the name of the individual accessing the data, along with the date and time of access, and the reason for the access.

- Audits shall be conducted at the discretion of the Chief of Police.

22.6.2 (ALPR) Sharing and Dissemination

- (ALPR) data can be accessed, retrieved, or shared, for

official and legitimate law enforcement operations or public safety purposes only.

- Information sharing among law enforcement agencies, other than the DCJIS, should be governed by departmental policies or memoranda of understanding.

22.6.3 Retention

- Bulk data from (ALPRs) will not be stored on the Department's server and will only be stored by LPD (ALPR) vendors. Either by their own protocols or at the direction of the Department, LPD (ALPR) vendors shall not store bulk Department (ALPR) data for a period greater than (30) days.

- Department (ALPR) data may be downloaded and retained by Department personnel in accordance with legitimate law enforcement purposes including specific investigations. This data shall be retained in accordance with MA Public Records laws and maintained until a final disposition has been reached in the particular case.

22.7: POLICY REVIEW

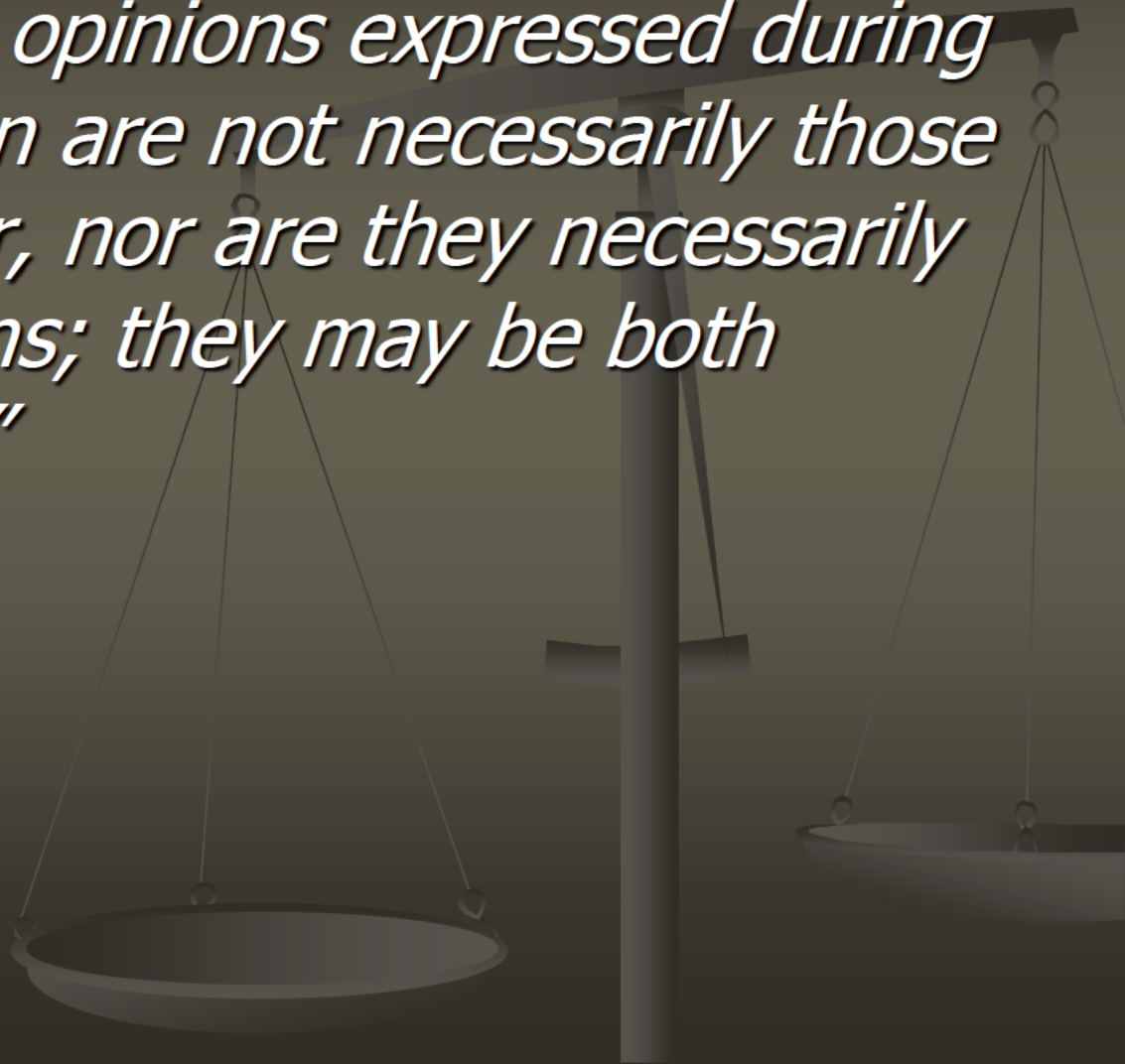
The (ALPR) Administrator is responsible for the annual review of this Policy and the policies and procedures contained herein and for making recommendations to the Department head for any necessary amendments. This is a new technology and it may raise both legal and technological issues. As use of the technology progresses, the Department will continue to monitor and assess the appropriateness of this Policy.

BERGEN COUNTY AUTOMATED LICENSE PLATE READER PROJECT

Assistant Prosecutor Martin Delaney
201-226-5806
mdelaney@bcpo.net
June 2012

DISCLAIMER

"The views and opinions expressed during this presentation are not necessarily those of the presenter, nor are they necessarily views or opinions; they may be both and/or neither."



INTERPRETING THE ATTORNEY GENERAL'S GUIDELINES

Plain Reading of the Guidelines; *plus*

Drafters' Intent.

Guidelines state all questions shall be address to the AG or his/her designee.

However, unless and until the courts get involved in interpreting the search & seizure ramifications of ALPR use, the answers are at best, educated speculation.

JUDICIAL REVIEW OF SEARCH & SEIZURE ISSUES



Law Enforcement's Need to Protect Public Safety

vs.

The Public's Legitimate Privacy Interest

JUDICIAL REVIEW

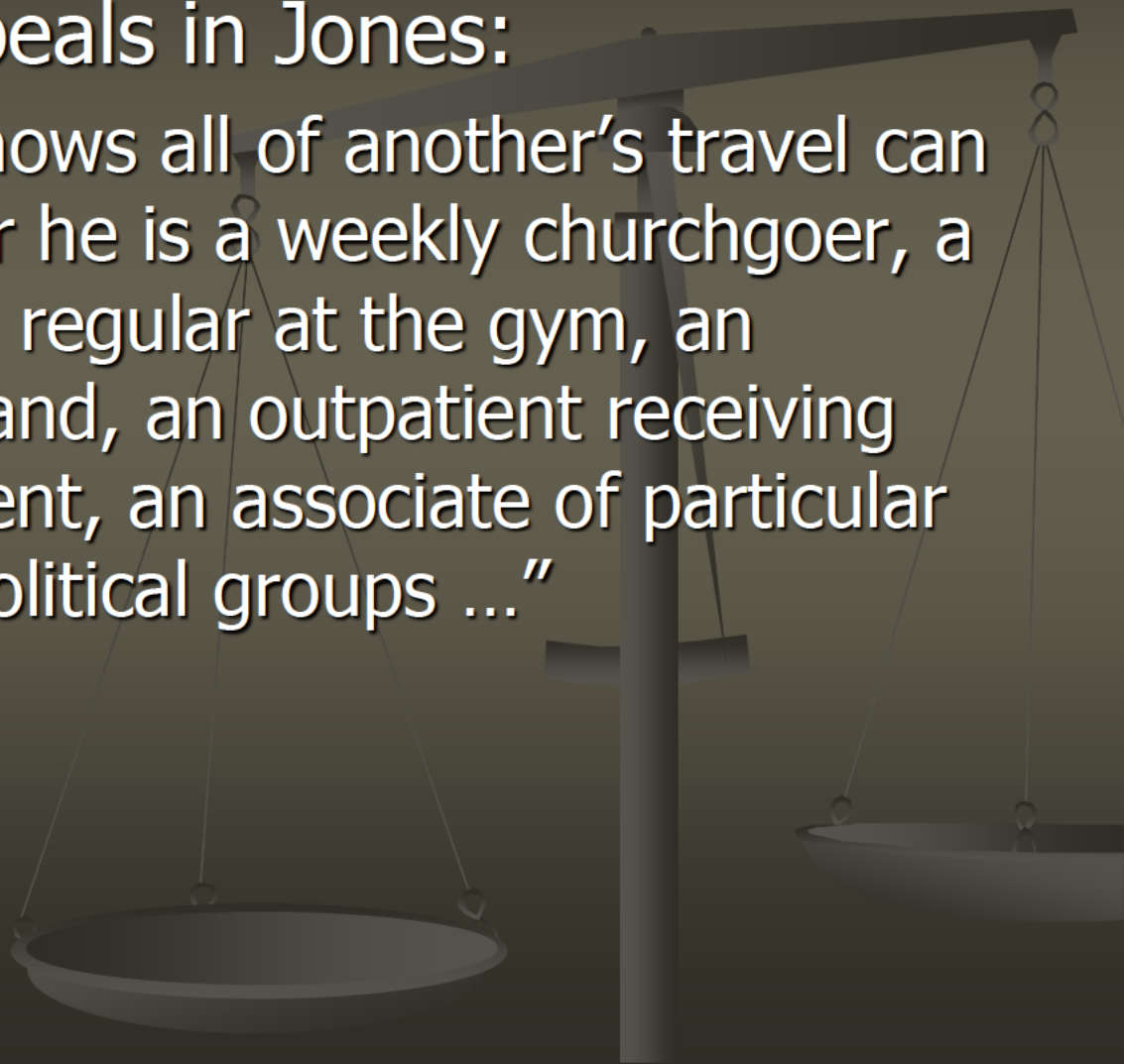
- **Unites States v. Jones** (No. 10-1259)

  In November 2011 the US Supreme Court heard a case to decide if the US Constitution requires police to obtain a warrant to attach a GPS device to a suspect's car and track its movements.

JUDICIAL REVIEW

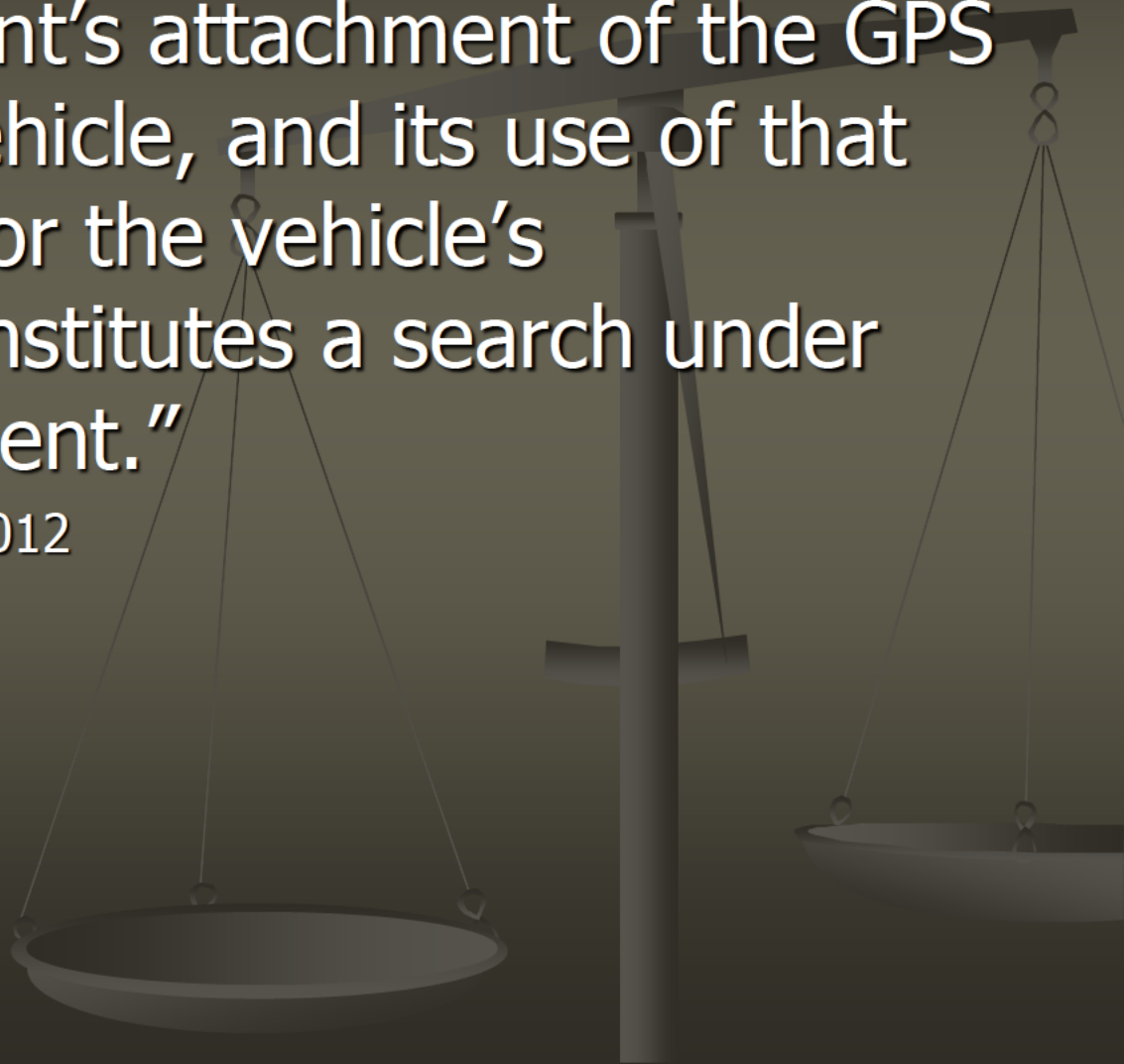
- US Court of Appeals in Jones:

  "A person who knows all of another's travel can deduce whether he is a weekly churchgoer, a heavy drinker a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups …"



US Supreme Court

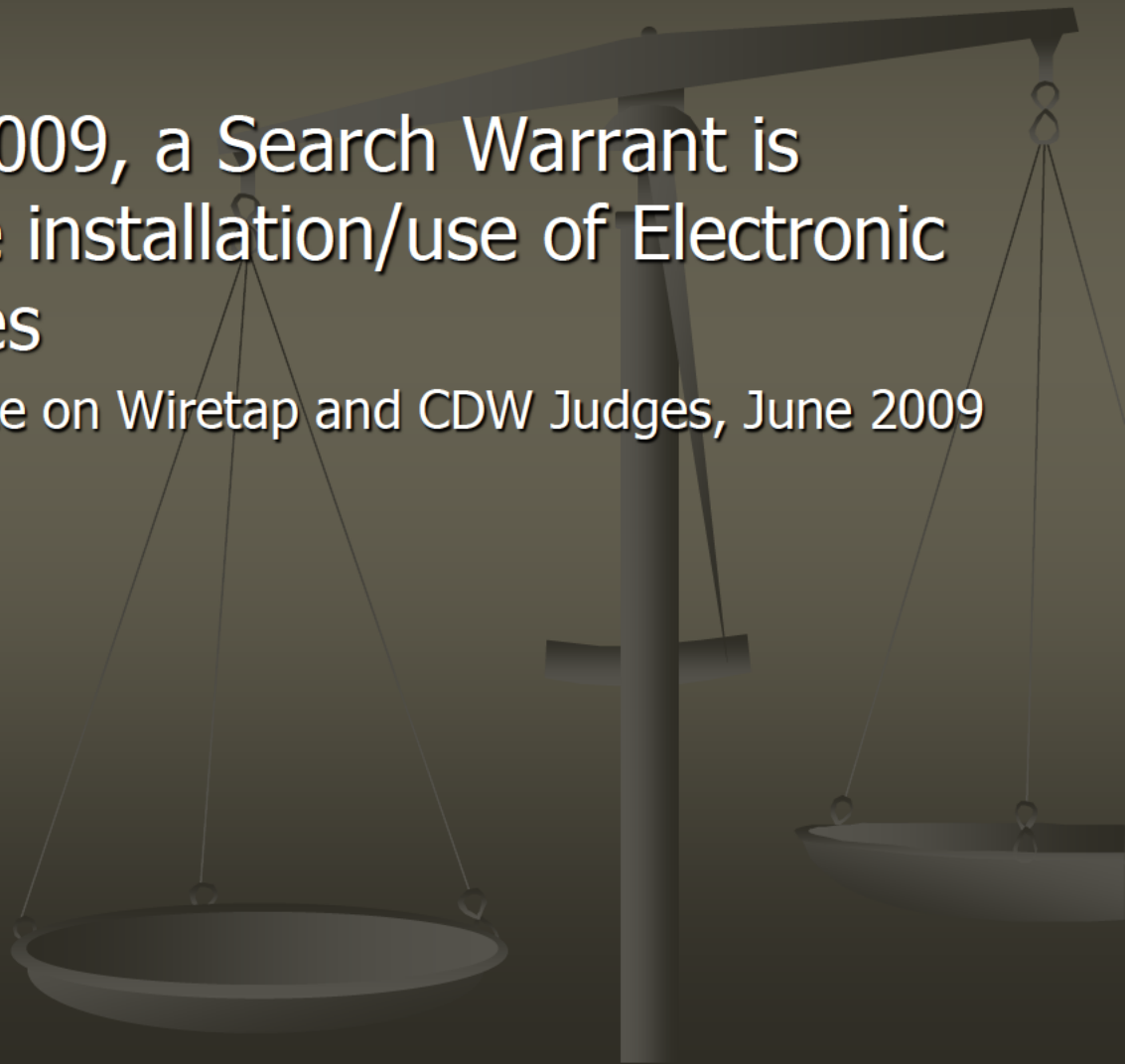
- "The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the 4th Amendment."
  - January 23, 2012



JUDICIAL REVIEW

New Jersey:

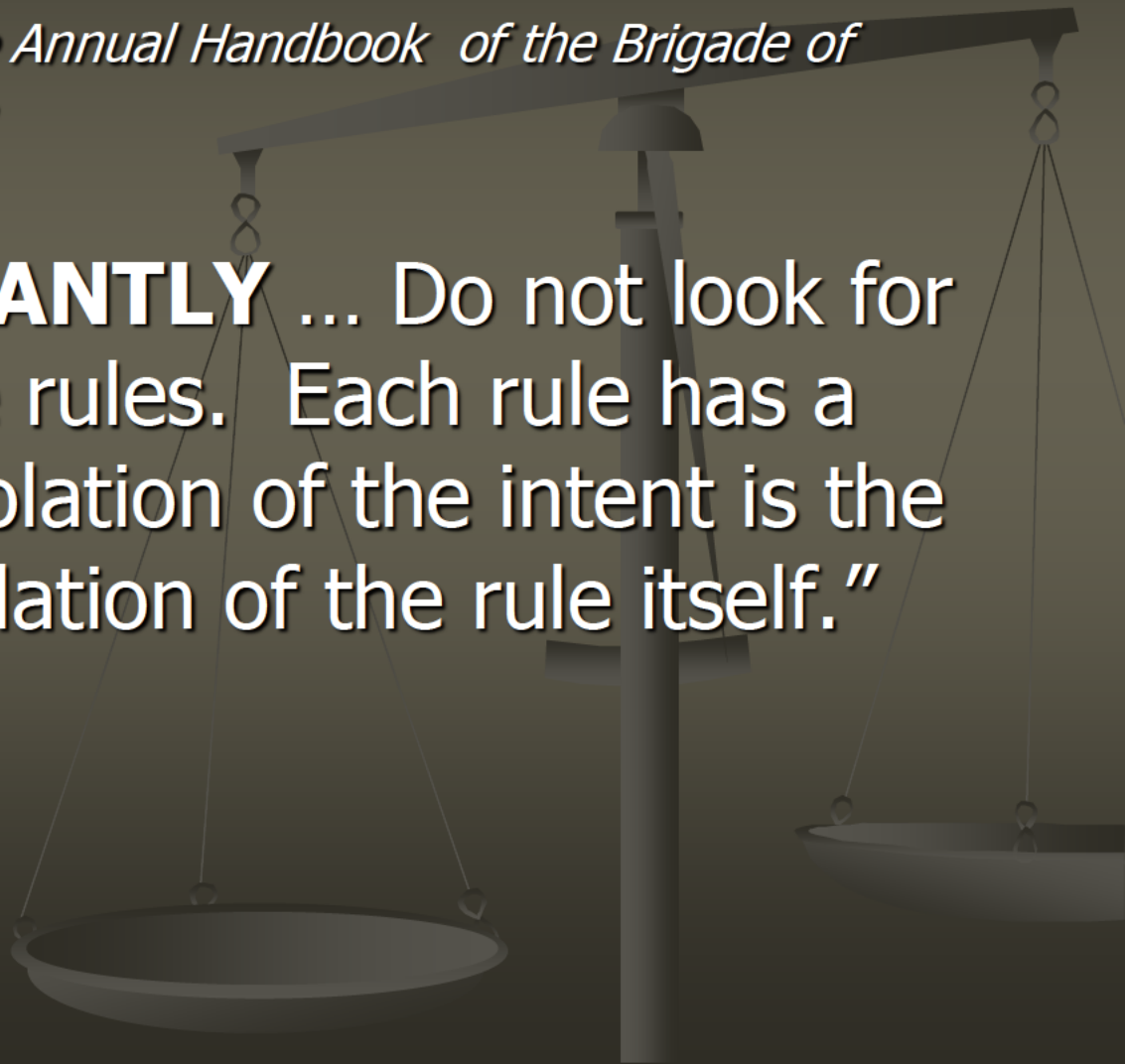
- Since at least 2009, a Search Warrant is required for the installation/use of Electronic Tracking Devices
  - Conference on Wiretap and CDW Judges, June 2009



DRAFTERS' INTENT & PLAIN READING

REEF POINTS, *The Annual Handbook of the Brigade of Midshipmen 100th Edition*

"**MOST IMPORTANTLY** … Do not look for loopholes in the rules. Each rule has a clear intent. Violation of the intent is the same as the violation of the rule itself."



DRAFTERS' INTENT

- ALPR technology supports the law enforcement mission.
- Guidelines are to ensure that "ALPRs are used only for *bona fide* law enforcement purposes."
- Also to "protect the legitimate privacy interests of motorists …" (*repeated throughout*).
- Guidelines provide for discipline/sanctions for any user who knowingly violates the guidelines.

PLAIN READING

- Each department must promulgate its own policy consistent with the AG's guidelines.
- North Arlington's policy was used as a template and conformed to fit both the AG's guidelines & the Bergen County system.

GUIDELINES/POLICY HIGHLIGHTS

- Section 1 Purpose & Scope:
  - emphasize throughout the importance of protecting privacy rights.
- Section 2 Definitions:
  - "Criminal Event" refers to Indictable Crimes ONLY.
  - Includes conspiracies and attempts, such as surveillance, planning and rehearsing, and/or the identification of security measures.

GUIDELINES/POLICY HIGHLIGHTS

- Section 3 Deployment of ALPR:
  - ONLY used by chief-authorized individuals;
  - Authorized user may be sworn officers and/or civilian employees;
  - Prior to use, all users must be trained in proper use of the ALPR system; and
  - Operation/Access is controlled by a secure, person-specific, log-on user identification and password.

GUIDELINES/POLICY HIGHLIGHTS

- Section 3 Deployment of ALPR:
  - Operation/Access is controlled by a secure, person-specific, log-on user identification and password.
  - Shall not be shared, transferred or used by any other individual(s).
  - Sharing log-in ID is a violation of the policy!

GUIDELINES/POLICY HIGHLIGHTS

- Section 4 Maintenance of Records:
  - BCPO maintains all ALPR records.
  - Records maintained for 5 years.
  - Subject to random audits.

We do it for you, but all recordation is based upon the proper use of the individual user's secure, person-specific, log-on user identification and password.

GUIDELINES/POLICY HIGHLIGHTS

- Section 5 Content & Approval of BOLO Lists:
  - Entering a plate number (or partial) requires a *legitimate & specific law enforcement reason* to:
    - Identify or locate the vehicle; or
    - Identify or locate any person who is reasonably related with the vehicle.

GUIDELINES/POLICY HIGHLIGHTS

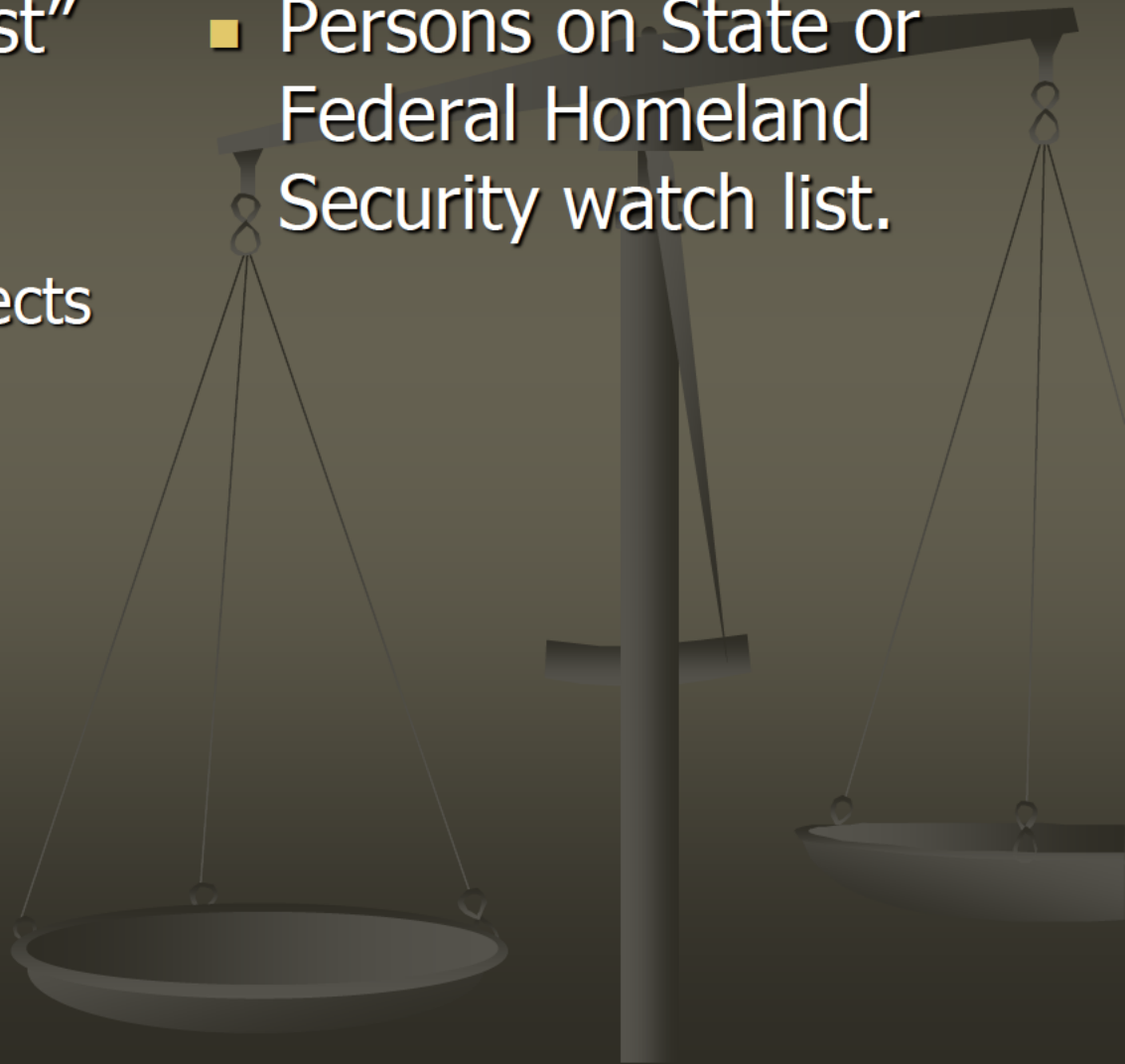
- Section 5 Content & Approval of BOLO Lists:
  - Post-scan of a plate number (or partial) requires a *legitimate & specific law enforcement reason* to:
    - Identify the past locations of the vehicle; or
    - Identify the past locations of any person who is reasonably related with the vehicle.

Legitimate & Specific Reasons

- Person who are subject of outstanding arrest warrants.
- Missing Persons.
- AMBER alerts.
- Stolen vehicles.
- Vehicles involved in crimes or disorderly persons offenses.
- Vehicles operated by unlicensed, revoked or suspended drivers.
- Vehicles with expired registrations or other Title 39 violations.
- Individuals subjected to restricted movements (curfew, TRO, Parole, etc…)

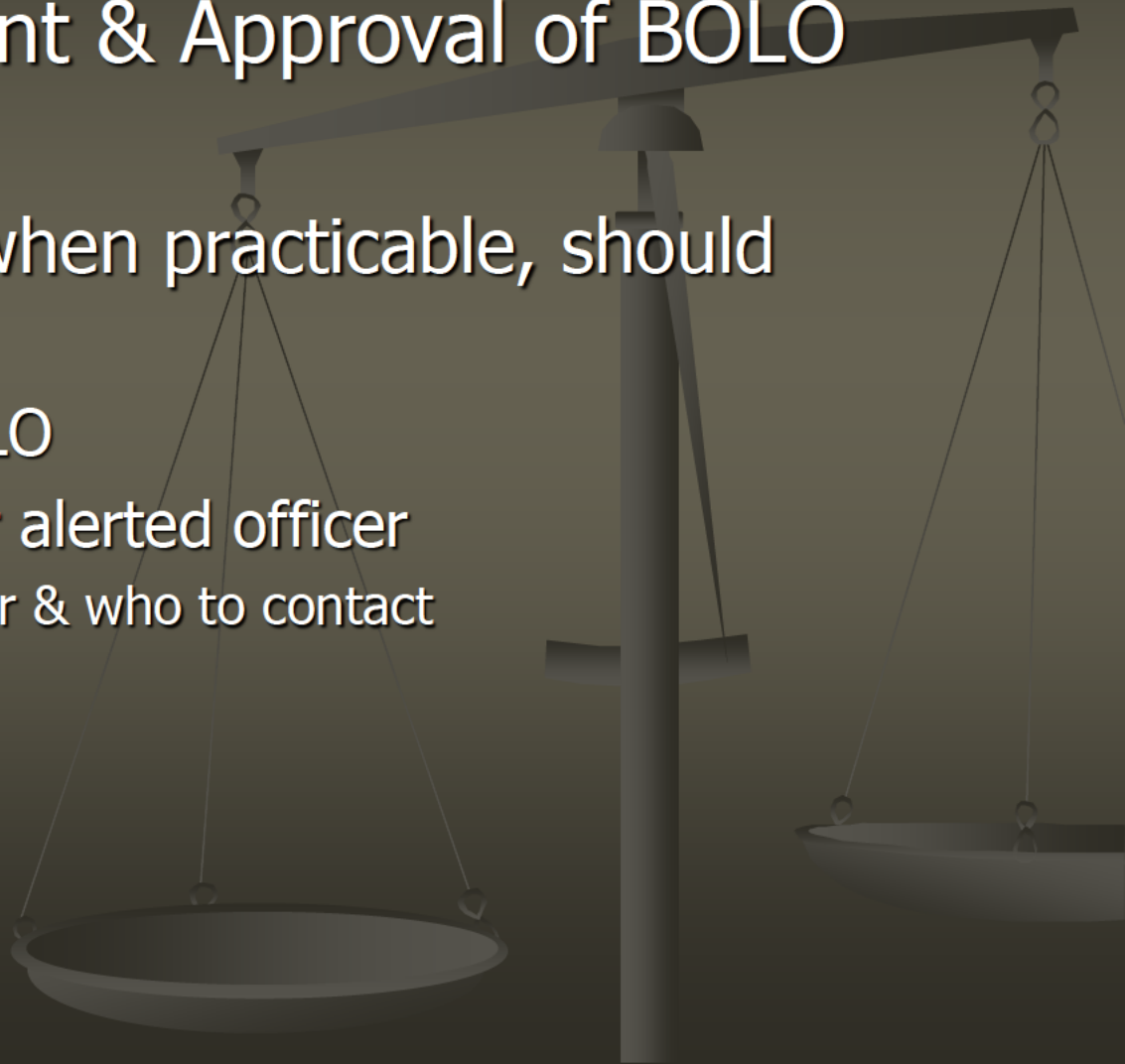
Legitimate & Specific Reasons

- "Persons of interest" in a specific investigation.
  - Need not be suspects themselves.
- Persons on State or Federal Homeland Security watch list.



GUIDELINES/POLICY HIGHLIGHTS

- Section 5 Content & Approval of BOLO Lists:
  - BOLO entries, when practicable, should include:
    - Reason for BOLO
    - Instructions for alerted officer
      - Non-Encounter & who to contact



GUIDELINES/POLICY HIGHLIGHTS

- Section 6 Police Action to Alert:
  - Alert alone may not justify police action!
  - Officer shall take appropriate actions given the circumstances.
    - i.e., take reasonable effort to confirm wanted individual is actually in the vehicle.

GUIDELINES/POLICY HIGHLIGHTS

- Sections 7 & 8 Security, Retention & Purging of ALPR Data:
  - BCPO is responsible for all aspects of these sections.

We do it for you, but all recordation is based upon the proper use of the individual user's secure, person-specific, log-on user identification and password.

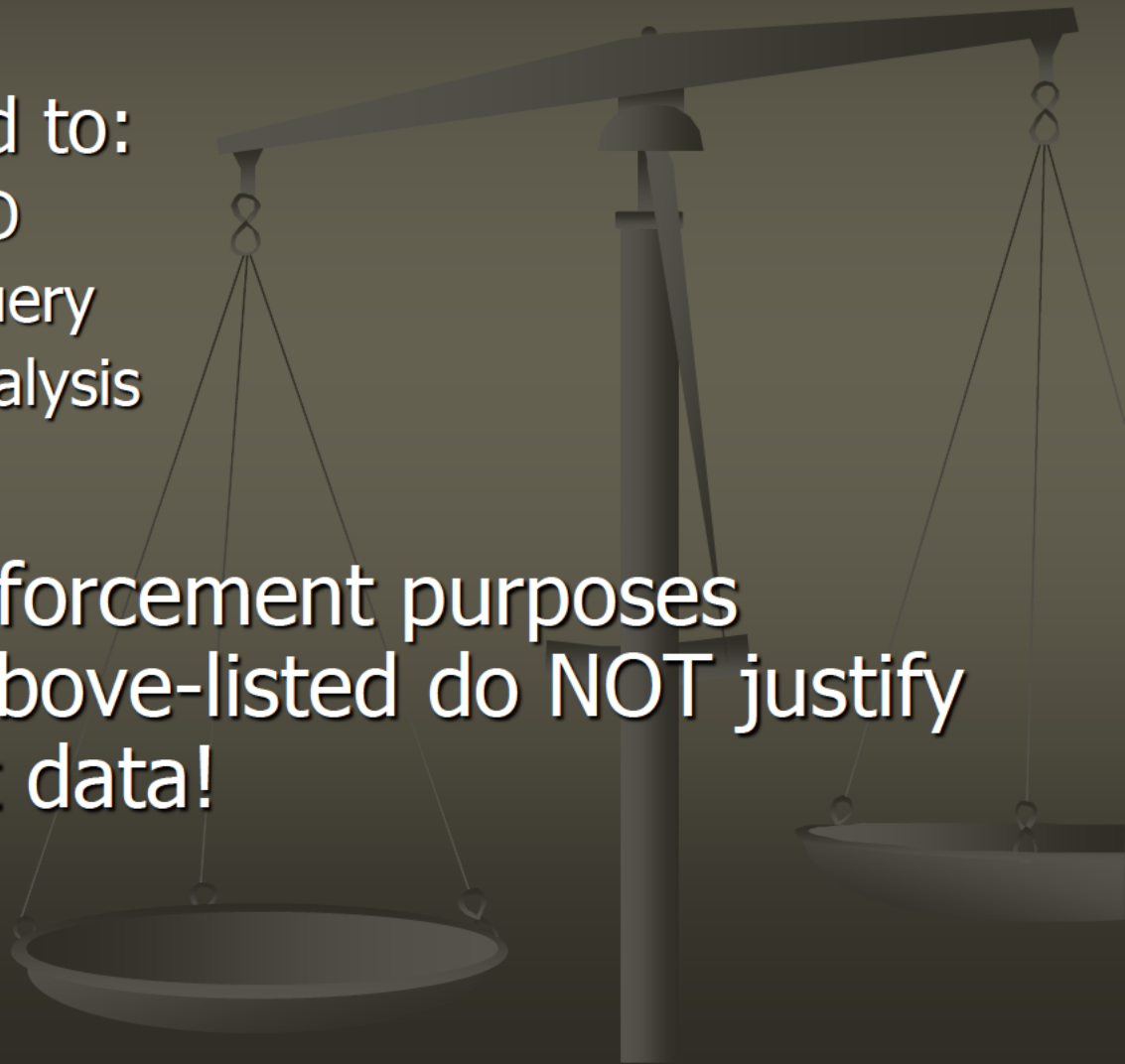
ACCESS & USE OF STORED ALPR DATA

- Positive Alert Data:
  - Authorized user may access for purposes of:
    - Post-scan BOLO query
    - Crime scene query
    - Crime trend analysis, via BCPO
    - Any other legitimate law enforcement purpose (whether part of an active investigation or not).

ACCESS & USE OF STORED ALPR DATA

- Non-Alert Data:
  - Access is limited to:
    - Post-scan BOLO
    - Crime-scene query
    - Crime trend analysis

Legitimate law enforcement purposes outside of the above-listed do NOT justify use of non-alert data!



NON-ALERT DATA & POST-SCAN BOLO QUERY

- Post-Scan BOLO of Non-Alert Data:
  - Authorized user may compare post-scan BOLO where query results might reasonably lead to:
    - Evidence/information related to investigation or law enforcement operation; or
    - When vehicle might be added to an active BOLO list.

(Ex: vehicle present at location to confirm or dispel an alibi defense.)

NON-ALERT DATA & POST-SCAN CRIME SCENE QUERY

- Crime Scene Query of Non-Alert Data:
  - Defined: accessing/reviewing stored ALPR data scanned at or about time/location or a reported *criminal event* to identify vehicles/persons associated as suspects, victims and/or witnesses.
  - Reasonably lead to evidence/information relevant to a *specific criminal event*.

NON-ALERT DATA & POST-SCAN CRIME SCENE QUERY

- Crime Scene Query of Non-Alert Data:
  - May not be reviewed for general crime patterns (who's in a high crime area?)
  - User must document the specific crime being investigated.
  - Review must be limited in scope to the event
    - Terrorist attack may justify weeks/months of review; a spontaneous crime may not

NON-ALERT DATA & CRIME TREND ANALYSIS

- Crime Trend Analysis Defined:

  "…stored ALPR data is used … to detect crime patterns by studying & linking common elements of recurring crimes …"

  and/or

  to predict when & where future crimes may occur; and/or

  to link specific vehicles to potential crimes or terrorist activity.

NON-ALERT DATA & CRIME TREND ANALYSIS

- Authorized user may access for crime trend analysis only if:

  Authorized by a trained supervisor (can be a standing order); and

  Where results of analysis are ***intended (not expected)*** to assist in the performance of the department's duties.

  Can include, if supervisor authorized, the use of automated software.

NON-ALERT DATA & CRIME TREND ANALYSIS

- SHALL NOT RESULT IN THE DISCLOSURE OF PERSONAL TO ANY AUTHORIZED USER … UNLESS:

(1) Authorized by Grand Jury subpoena; or

(1) Specific & Articulable facts of the analysis warrant further investigation; and

(2) A supervisor approves the release of the identifying information.

NON-ALERT DATA & CRIME TREND ANALYSIS

1337

- Authorized user accessing stored non-alert data for crime scene trend analysis shall document:
  - Nature & purpose of the analysis;
  - Identity of the person accessing data; and
  - Identity of the authorizing supervisor.

NON-ALERT DATA & CRIME TREND ANALYSIS

- Additionally, where there is disclosure of identifying information, user must document:
  - The facts warranting the disclosure;
  - Identity of the authorizing supervisor; and/or
  - The existence of the grand jury subpoena.

SHARED LAW ENFORCEMENT ACCESS TO STORED ALPR DATA

- May be shared and provided to any other ***law enforcement agency***.
- All sharing of information must be recorded:
  - Agency; and
  - Individual to whom information was provided.

SHARED NON-LAW ENFORCEMENT ACCESS TO STORED ALPR DATA

- Shall NOT be provided, unless:
  - Authorized by subpoena or court order
    - Prior to release notify Chief & Prosecutor;

    or
  - Required by the Rules of Court – discovery.

THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

OFFICE OF THE ATTORNEY GENERAL
ATTORNEY GENERAL MAURA HEALEY



A PROJECT OF THE CRIMINAL BUREAU
DIGITAL EVIDENCE LABORATORY
APPEALS DIVISION

JUNE 2021

A NOTE TO READERS OF THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

The Massachusetts Digital Evidence Guide (hereinafter "Guide") is only to be used as an educational resource. This Guide is not legal advice. The purpose of this Guide is to provide the reader with an understanding of the Massachusetts statutes and cases impacting criminal investigations and prosecutions that involve technology or digital evidence. This Guide, and its provisions, are not policy. This Guide does not suggest modifying or replacing any existing agency practices or procedure(s). Readers should consult with appropriate authorities, prosecutors, or legal counsel for necessary legal advice, case or statutory interpretation, or implementation of the document for any internal use. Readers who intend to rely on cases and statutes cited in this Guide should consult with the source document, confirm the interpretation, and investigate subsequent history. Questions or comments about, or suggestions for this Guide can be e-mailed to agodel@mass.gov.

THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

Office of the Attorney General, Maura Healey

Contents

Contents 2

I. Investigation 7

A. The Search and Seizure of Digital Evidence 7

1. Was There a Search or Seizure? 7

a) Searches and the Reasonable Expectation of Privacy 8

(1) Standing 8

(2) One Party Consent 9

(3) The Third-Party Doctrine 9

(4) Surveillance in Public: Public View Principle, Mosaic Theory, and More 13

(5) Peer-to-Peer and Other Network File Sharing 14

(6) Expectation of Privacy in Data That Is Not One's Own 16

(7) Probationers, Parolees, and Court-Ordered Monitoring 17

b) Seizures and Interference with Possessory Interest 19

c) Private Party Searches 20

(1) Initial Search Made by Private Party 20

(2) Warrantless Search: Private Citizen or State Actor 21

(3) An ISP's Reporting Obligation Does Not Make it a State Agent 22

2. Was a Search or Seizure Reasonable? 22

a) Warrants 22

(1) Probable Cause / Affidavit 23

(2) Independent Source Doctrine 30
(3) Particularity / Scope 31
(4) Staleness of Information Supporting Probable Cause 36
(5) Timely Execution of the Warrant 38
(6) Manner of Executing the Warrant 39
b) Exceptions to the Warrant Requirement 40
(1) Search Incident to Arrest 40
(2) The Plain View Doctrine 42
(3) Exigent Circumstances 44
(4) Emergency Aid Exception 45
(5) Inventory Exception 46
(6) Consent 47
3. The Exclusionary Rule 48
a) Good Faith / Substantial and Prejudicial 48
b) Inevitable Discovery 49
B. Search of Electronic Service Providers 49
1. General Overview of Stored Communications Act 49
2. Search warrants served on out-of-state Internet service providers 50
C. Encryption and Self Incrimination 50
1. The Foregone Conclusion Doctrine 50
2. Encryption 51
3. Sample Decryption Protocol 54
D. Searches Implicating Attorney-Client Privilege 54
1. Post-Indictment Email and File Searches 55

2. Taint Teams 55
3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails) 56
II. Evidentiary Matters 57
A. Judicial Discretion 57
1. Trial Judge's Discretion 57
2. Demonstrative Photographs 57
B. Discovery 57
1. Pornographic Images in Child Pornography Cases 57
2. Wiretap transcripts 58
3. Cell phone data 58
C. Authentication 59
1. Generally 59
2. Photographs and Digital Images, Videos, and CDs 59
3. Digitally Enhanced Images and Video 60
4. Transcripts of Recordings 60
5. Email 61
6. Chatrooms 62
7. Text Messages 62
8. Information Available on Websites and Social Networks 62
9. Software Programs Used in Investigation 64
10. GPS and Probation 64
D. Technological evidence as the basis of criminal conviction 65
E. Best Evidence Rule 66
1. Best Evidence Rule - Generally 66
2. Digital Images 66

3. Admission of Duplicate Evidence 66
4. Videos 67
5. Email 67
6. Summaries 67
F. Hearsay 68
G. Business Records Exception 68
1. Email 68
2. Computer Records 69
H. Confrontation Clause 69
1. Software-generated information 69
2. Secondary Examiners 70
III. Cybercrimes 72
A. Possession of Child Pornography 72
1. Multiple Convictions Require Multiple "Caches" 72
2. Brief Possession is Sufficient 72
3. Receipt by Cell Phone is Sufficient 73
4. Malware and Computer Viruses Defense 73
5. Probable cause / Staleness in Child Pornography Cases 73
B. Statutory Terms of Mass Gen. Laws ch. 272 74
1. "Dissemination" 74
2. Computer "Depictions" 74
3. Child Enticement 75
4. "Visual Material" 75
5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31 75
6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A 75

7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A 76
8. Lewdness 77
C. Special Conditions of Probation 77
IV. Expert Testimony About Technology 79
V. List of Cases Organized by Device/Evidence Type 80
A. Cell Phone Searches 80
B. Search of Computer Files 80
C. Email 80
D. CSLI, GPS, and Other Location Technologies 81
E. Text Messages 81

I. Investigation

A. The Search and Seizure of Digital Evidence

As with physical evidence, searches and seizures of digital evidence must be reasonable to be valid. This section provides a summary of Fourth Amendment law as it relates to the search and seizure of digital evidence. It also references Article Fourteen of the Massachusetts Declaration of Rights, which parallels the Fourth Amendment, but is sometimes more expansive.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Article Fourteen (art. 14) of the Massachusetts Declaration of Rights is similar to the Fourth Amendment, but since 1985, the Supreme Judicial Court ("SJC") has interpreted it as providing broader protections than its federal counterpart. Commonwealth v. Upton, 394 Mass. 363, 373 (1985) ("We conclude that art. 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause.").

To determine whether law enforcement action constitutes an unreasonable search or seizure, courts ask two questions. First, was the action a search or seizure within the meaning of the Fourth Amendment? E.g., Commonwealth v. Magri, 462 Mass. 360, 366 (2012) ("In deciding whether police conduct violates the Fourth Amendment or art. 14 of the Massachusetts Declaration of Rights, we first determine whether a search, in the constitutional sense, has taken place."). Second, was that search or seizure reasonable? See, e.g., Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness." (internal quotation marks omitted)).

1. Was There a Search or Seizure?

"A search implicating the Fourth Amendment occurs 'when an expectation of privacy that society is prepared to consider reasonable is infringed' and a seizure of property for purposes of the Fourth Amendment occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'" Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (quoting United States v. Karo, 468 U.S. 705, 712 (1984)) (finding installation and use of a GPS tracking device on a car to be a seizure under Massachusetts art. 14 because it requires entering the vehicle and using the electricity of the defendant's car).

a) Searches and the Reasonable Expectation of Privacy

For a search to implicate the Fourth Amendment, the defendant must have a "reasonable expectation of privacy" in the place to be searched. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); see also United States v. Heckencamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding a college student had a reasonable expectation of privacy in the contents of his personal computer because it was located in his dorm room, was protected by a password, and was not subject to regular university monitoring). A person's expectation of privacy is reasonable "if he can demonstrate a subjective expectation that his activities would be private, and he can show that his expectation was one that society is prepared to recognize as reasonable." Heckencamp, 482 F.3d at 1146 (internal quotation marks, brackets, and citations omitted). Individuals generally have a reasonable expectation of privacy in their personal computers and files. See id. at 1146–47 (listing cases to that effect). In Heckencamp, "[t]he salient question [was] whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network." Id. at 1146.

When challenging the constitutionality of a search, the defendant bears the initial burden of establishing that a search occurred. See Commonwealth v. D'Onofrio, 396 Mass. 711, 714-15 (1986); Commonwealth v. Alvarez, 480 Mass. 1017, 1018 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer).

The sections below explore the contours of the reasonable expectation of privacy, discussing: (1) standing; (2) one-party consent; (3) the third-party doctrine; (4) surveillance in public; (5) file sharing over networks; (6) reasonable expectations of privacy in data that is not one's own; and (7) diminished privacy expectations in the context of probationers, parolees, and court-ordered monitoring.

(1) Standing

Standing to challenge a warrantless search or seizure may be in question when the location or item searched or seized does not belong to the challenging party.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully suppressed CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105, 107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Commonwealth v. Almonor, 482 Mass. 35 (2019), the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Almonor, 482 Mass. at 47-48 (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The Court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have

automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because, "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Id. at 108. The Court found that the defendant did have standing to challenge the search of his own cell phone, but the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 108-09.

(2) One Party Consent

In Massachusetts, "one party consent" does not negate a reasonable expectation of privacy of the non-consenting party. While the Supreme Court held that warrantless electronic surveillance with "one party consent" does not implicate the Fourth Amendment, United States v. White, 401 U.S. 745, 751 (1971), the SJC found such surveillance impermissible under art. 14 of the Massachusetts Declaration of Rights, Commonwealth v. Blood, 400 Mass. 61, 70 (1987). Because it found there is a reasonable expectation of privacy in conversations that occur among "a narrow compass of known listeners" in private homes, the SJC concluded that the warrantless electronic surveillance was a violation of that constitutional provision. Id. Accordingly, "one party consent" did not obviate the need for a warrant under art. 14. Id.

(3) The Third-Party Doctrine

In United States v. Miller, 425 U.S. 435 (1976), and Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court articulated what has become known as the "third-party doctrine." Under this doctrine, "the Fourth Amendment does not prohibit the obtaining of information revealed [by a suspect] to a third party and conveyed by him to Government authorities," regardless of the suspect's expectation of how the information might be used. Miller, 425 U.S. at 443. Massachusetts has traditionally followed the Supreme Court's guidance on the third-party doctrine. See, e.g., Commonwealth v. Cote, 407 Mass. 827, 833–36 (1990) (holding that a defendant had no reasonable expectation of privacy in telephone message records held by a third-party answering service for the reasons cited in Miller).

- United States v. Jones, 565 U.S. 400 (2012). Unanimous decision holding that a Fourth Amendment "search" occurs where law enforcement places a GPS device on defendant's car. Id. at 411. The Court's opinion, authored by Justice Scalia, focused on the Government's intrusion on the defendant's physical property and applied "an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted." Id. In contrast, Justice Sotomayor's concurrence in Jones emphasized that "the Fourth Amendment is not concerned only with trespassory intrusions on property," id. at 954, and brought the issues later addressed by Carpenter v. United States, 138 S. Ct. 2206 (2018), to the forefront, see Jones, 565 U.S at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age…").

Carpenter v. United States, 138 S. Ct. 2206 (2018) and Commonwealth v. Augustine, 467 Mass. 230 (2014) modified the third-party doctrine for at least one specific type of information—cell site location information ("CSLI"). The holding of Carpenter is that law enforcement effects a Fourth Amendment "search" by obtaining at least one week's worth of a defendant's CSLI from a third-party cellular provider. See Carpenter, 138 S. Ct. 2206, 2217 n.3. The comparable holding from Augustine is that subpoenaing two weeks' of CSLI information is a "search." See Augustine, 467 Mass. 230, 233, 255 (2014).

- Carpenter v. United States, 138 S. Ct. 2206 (2018). The Government successfully applied for two court orders directing Carpenter's wireless carriers to disclose Carpenter's CSLI for select time periods within a four-month span. 138 S. Ct. at 2212. The first order sought 152 days of CSLI from MetroPCS, and the second order sought seven days of CSLI from Sprint. Id. Based in part off the information the Government acquired from Carpenter's CSLI, the Government charged Carpenter with six counts of robbery and six counts of carrying a firearm during a federal crime of violence. Id.

  The Supreme Court held that the Government's acquisition of Carpenter's CSLI was a search of Carpenter that required a warrant supported by probable cause even though the Government acquired the CSLI from third-party wireless carriers. Id. at 2221. The Court declined to apply an expansive version of the third-party doctrine to CSLI partly because the data can reveal immense amounts of intimate information about who a suspect has been associating with and where a suspect has been travelling. Id. at 2219 ("There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today."). Furthermore, because cell phones are a nearly ubiquitous part of daily life and virtually every activity on a phone generates CSLI, the Court rejected the claim that Carpenter voluntarily disclosed his CSLI to his wireless carriers. Id. at 2220 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term.").

  While the Court stated that its ruling was "a narrow one" that applied only to CSLI, id., the dissents argued that the decision will have far-reaching consequences, e.g., Carpenter, at 2234 (Kennedy, J., dissenting) ("The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties."); see also id. at 2262 (Gorsuch, J., dissenting) ("Today the Court suggests that Smith and Miller distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to 'extend' those decisions to particular classes of information, depending on their sensitivity." (emphasis in original)); cf. Commonwealth v. Augustine, 467 Mass. 230, 253 (2014) (holding that although "we do not reject categorically the third-party doctrine," some forms of electronic evidence require "a different approach"). Given Americans' increasing dependence on technological devices that generate large amounts of personal data, it is possible that the Supreme Court's reasoning in Carpenter will someday result in a larger overhaul of the third-party doctrine.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case similar to Hobbs, considering retroactive application of Augustine's warrant requirement for CSLI data, the SJC again held constitutional a pre-Augustine CSLI request because the associated 18 U.S.C. § 2703 application satisfied the requisite probable cause standard. Id. at 166-72.

- Commonwealth v. Almonor, 482 Mass. 35 (2019). This case concerned an issue of first impression involving whether police action that causes an individual's cell phone to transmit its real-time location information violates any reasonable expectation of privacy. Id. at 41. Neither the Supreme Court's decision in Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018) nor the SJC's decision in Commonwealth v. Augustine, 467 Mass. 230, 4 N.E.3d 846 (2014) addressed this precise issue. The Commonwealth charged the defendant with murder after he shot and killed an individual and subsequently fled the scene of the crime. After a witness gave them the defendant's phone number, the police filed a "mandatory information for exigent circumstance requests" form with the telephone service provider. The telephone service provider "pinged" the defendant's phone and revealed the defendant's GPS coordinates to the police. Id. at 38-39. The Court granted the defendant's motion to suppress the warrantless "pinging." Id. The SJC reversed, holding that the warrantless pinging of the defendant's phone constituted a search under the Article 14 of the Massachusetts constitution, but that the warrantless search was justified by exigent circumstances, namely that the defendant was at large and believed to be armed and dangerous. It noted that searches occur when the government intrudes on a person's reasonable expectation of privacy and concluded that the defendant had a reasonable expectation of privacy in his cellular location data. Id. at 43-44. The Court held that real-time location data serves as a "proxy for the real-time location of the individual" because "cell phones are an indispensable part of daily life and exist as almost permanent attachments to their users' bodies." Id. at 45 (internal quotations omitted).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). In 2011, the government received historical CSLI from defendant's cell service provider pursuant to a 18 U.S.C. § 2703 order, without a warrant — well before 2014, when Augustine first articulated the warrant requirement for historical CSLI requests. Id. at 542-44. The SJC held that the government could "still satisfy the warrant requirement if it can establish that its 'application for the § 2703[] order met the requisite probable cause standard of art. 14,'" i.e., the same probable cause standard required of an affidavit in support of a search warrant for historical CSLI. Id. at 544 (quoting Augustine, 467 Mass. at 256). (This also comports with Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016), an earlier case considering retroactive application of Augustine to CSLI data obtained pre-Augustine pursuant to an 18 U.S.C. § 2703 order.)

- Commonwealth v. Fulgiam, 477 Mass. 20 (2017). In Fulgiam, the Commonwealth obtained recent text messages of the defendant pursuant to § 2703(a) of the Federal Stored Communications Act. Id. at 28; 18 U.S.C. § 2703(a) (2012). The Court held, on federal statutory and state constitutional grounds, that law enforcement required a warrant to obtain the text messages. See 477 Mass. at 31. An individual under Massachusetts state law has a "reasonable expectation of privacy in his text messages." Id. at 33. The third-party doctrine did not require

otherwise because "the nature of cellular telephone technology . . . [and] use in our current society render the third-party doctrine inapposite" in this context. Id. at 34.

- Commonwealth v. Estabrook, 472 Mass. 852 (2015). The SJC considered a request for CSLI and concluded that a defendant's reasonable expectation of privacy under art. 14 of the Massachusetts Declaration of Rights is not violated by a warrantless request for production of up to six (6) hours of historical CSLI. Id. at 854. It also established that the relevant consideration in determining the reasonable expectation of privacy is the length of time for which CSLI data is requested, not the time span ultimately sought to be introduced at trial. Id. at 858–59.

- Commonwealth v. Augustine, 467 Mass. 230 (2014). Police investigating a murder obtained the defendant's CSLI from his service provider pursuant to a 18 U.S.C. § 2703(d) order. Id. at 233. These orders are not warrants, so they cannot be used to effectuate a search for information protected by the Fourth Amendment or art. 14. The CSLI obtained helped police determine the defendant's location over the period they were investigating. See id. at 233–34. The Court considered but ultimately rejected the Commonwealth's argument that the third-party doctrine negated any reasonable expectation of privacy the defendant had in his CSLI. Id. at 241–56. It reasoned that art. 14 does not protect information voluntarily and intentionally transmitted to third parties (like the number dialed to initiate a call) but it does protect information incidentally transmitted (like the location information the cell phone provider acquires as a result of cell phone technology). Id. at 249–52. The Court found that the defendant therefore had a reasonable expectation of privacy in his CSLI, which, under art. 14, means that "the government must obtain a search warrant to obtain it." Id. at 252.

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). Law enforcement obtained thousands of emails related to fraudulent marketing claims from the defendant's Internet Service Provider (ISP). Id. at 281. The defendant challenged such access to his email on Fourth Amendment grounds. Id. at 282. The Sixth Circuit agreed and held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" Id. at 288 (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)). In finding that a reasonable expectation of privacy existed in this case, the Sixth Circuit analogized email transmitted via ISP to the contents of telephone conversations and closed letters, each of which received Fourth Amendment protection. See id. at 286–87. Rebutting the third-party doctrine argument, the Sixth Circuit—similar to the SJC in Augustine above—noted that the ISP in this case was an *intermediary* rather than the intended target of a conversation. Id. at 288. Thus, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." Id. Though binding only in the Sixth Circuit, this case has been cited by some of the largest email providers in requiring warrants to obtain the contents of email. See Brendan Sasso, *Facebook, email providers say they require warrants for private data seizures*, The Hill (Jan. 25, 2013), http://thehill.com/policy/technology/279441-facebook-email-providers-require-warrant-for-private-data. The Department of Justice also requires its prosecutors nationwide to follow this holding.

(4) Surveillance in Public: Public View Principle, Mosaic Theory, and More

Under the "public view" principle, individuals generally do not have a reasonable expectation of privacy in items or places that they expose to the public. California v. Ciraolo, 476 U.S. 207, 213 (1986) ("[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares"). In particular, "the government, without… a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance." Augustine, 467 Mass. at 252. (Note that this principle as stated in Augustine is in some tension with the SJC's decision in Mora, as discussed below.)

Courts have limited the public view principle in "constitutionally sensitive" settings (epitomized by the home) where individuals have a strong expectation of privacy that society is prepared to recognize, especially where technology has enabled previously infeasible collection of information about the inside of a home via surveillance technology situated outside the home (i.e., in public). See Kyllo v. United States, 533 U.S. 27 (2001) (holding warrantless surveillance of heat levels inside a home using thermal-imaging equipment outside the home to be an unconstitutional search).

Recent developments suggest that courts are increasingly recognizing constitutional warrant requirements in more situations involving surveillance in public places, when such surveillance is particularly expansive and detailed, or implicates "constitutionally sensitive" domains such as the home. The SJC has recognized the "mosaic theory" or "aggregation principle for the technological surveillance of public conduct," under which "'the cumulative nature of… information collected [when collected over a long enough period] implicates a privacy interest on the part of the individual who is the target of the tracking,'" even when the individual activities or data points surveilled would not enjoy constitutional protection taken alone. Commonwealth v. McCarthy, 484 Mass.493, 503-04 (2020)(quoting Augustine, 467 Mass. at 253); see also Jones, 565 U.S. at 416 (Sotomayor, J., concurring).

- Commonwealth v. McCarthy, 484 Mass. 493 (2020). The Court considered the constitutionality of warrantless use of automatic license plate readers (ALPRs), which are "cameras combined with software that allows them to identify and 'read' license plates on passing vehicles." Id. at 494. Drawing on the "mosaic theory," the SJC stated that "[a] detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts," and noted that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." Id. at 504, 506. On the facts of the case, however, the SJC found no constitutional violation: "[T]he analysis should focus, ultimately, on the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance [at issue]. … [F]or this case, we consider the constitutional import of four cameras placed at two fixed locations… [and] conclude that the limited use of ALPRs in this case does not constitute a search within the meaning of either art. 14 or the Fourth Amendment." Id. at 506, 508,509.

Pole camera surveillance is a notable area where courts' approaches in applying the "public view" principle have been shifting recently, especially after Carpenter, 138 S. Ct. 2206, and Jones, 565 U.S. 400. While "[m]ost courts to have addressed pole camera surveillance have concluded that it does not infringe on any reasonable expectation of privacy" under the "public view" principle, "several courts have reassessed prolonged pole camera surveillance." Commonwealth v. Mora, 485 Mass. 360, 364-65 (2020) (citing as examples United States v. Vargas, No. CR-13-6025 (E.D. Wash. Dec. 15, 2014) (six weeks of pole camera surveillance was search); State v. Jones, 2017 S.D. 59 (2017) (two months was search); People v. Tafoya, 2019 COA 176 (Colo. App. 2019) (three months was search)). Mora is the most recent Massachusetts case on pole camera surveillance.

- Commonwealth v. Mora, 485 Mass. 360 (2020). Investigators installed pole cameras on public telephone and electric poles for the purpose of surveilling the defendants. Id. at 361. Most of the cameras were aimed at the homes of defendants or other individuals; one was aimed at a street that a defendant used to conduct his drug business. Id. at 362. The cameras had video but not audio recording capabilities, they could not view inside any residence, and they did not have infrared or night vision capabilities; however, investigators could remotely zoom and angle the cameras in real time. Id. The footage was stored in a searchable format that allowed officers to review previously-recorded events. Id. The SJC held that the pole camera surveillance of the defendants' homes was a warrantless search in violation of Article 14 of the Massachusetts Constitution. Id. at 370-76. Pole camera surveillance of public streets frequented by the defendants away from their homes was not subject to a warrant requirement, however, as defendants had no reasonable expectation of privacy in those locations. Id. at 369. The defendants' homes did not have fencing or other attempts to shield the residences from view, a fact that the court held immaterial to the constitutionality of surveillance. Id. at 366-67. The court noted that the Fourth Amendment might well require the same outcome, but declined to reach the federal constitutional question as the case could be resolved on state constitutional grounds. Id. at 361.

(5) Peer-to-Peer and Other Network File Sharing

The following cases illustrate when making data accessible to the public or certain networks via peer-to-peer file sharing techniques eliminates one's reasonable expectation of privacy.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Defendant was an instructor at a high school's electronics shop. Police officers remotely observed pirated movies and child pornography in an open share folder of a computer named Joester7437, which was connected to the school's network. Id. at 103–05. [Note: Joester7437 was later determined to belong to a student. Id. at 105.] While searching the school for Joester7437, the police found a computer/server named "Nightcrawler." Id. at 105. Nightcrawler's screen displayed an open share folder with the same pirated movie as was found on Joester7437. Id. "The source of the open share was Sinister, another unauthorized computer logged onto the high school's network." Id. The police found Sinister in the defendant's office, but that computer was password protected. Id. They seized Sinister "on probable cause to believe that it contained child pornography and copyrighted intellectual property." Id. They then received a search warrant for it based on an affidavit

alleging: (1) both shared folders (in Joester7437 and Sinister) had a copy of the same pirated movie, (2) Joester7437's open share folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 111. The defendant did not dispute that he had no reasonable expectation of privacy in files shared with the network. Id. at 107. Instead, the defendant argued that he did have a reasonable expectation of privacy in his *private* files and that there was no probable cause to search the private files for child pornography. Id. The Court held that the affidavit in support of the search warrant did not establish probable cause to believe that child pornography was located in the private files on the defendant's computer (Sinister). Id. at 111. The SJC noted: "None of these facts, even when considered together, provided a 'substantial basis' to believe that the defendant's private files contained child pornography." Id.

- Commonwealth v. Hay, 90 Mass. App. Ct. 1122 (2016) (unpublished). Defendant argued that the pre-warrant investigation was a "search" within the Fourth Amendment because the P2P [peer-to-peer] network was open only to a small group of known individuals, id. at *6, and because law enforcement used specialized SHA technology to identify a file on the defendant's computer that was likely to contain child pornography, id. at *7 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001) (government's use of device not in general public use "to explore details of the home that would previously have been unknowable without physical intrusion" is a search)). The appeals court held that, though it is possible that a file-sharing network open only to a small group of known individuals might give rise to a reasonable expectation of privacy in the files, the defendant had not argued or shown that the network in question here (Gnutella), as used with the specific software client used by the defendant (LimeWire), was such a network. Id. at *7. The appeals court also held the investigation was not a search because the defendant offered no evidence that the SHA technology enabled law enforcement to learn any more about the files than could any other P2P user. Id.

- United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010). Defendant shared child pornography over a peer-to-peer file sharing network that was being monitored by police using special forensic software. Id. at 1046–47. Police remotely downloaded the incriminating files from the defendant's folder on the peer-to-peer network. Id. at 1047. The Ninth Circuit held the defendant had no reasonable expectation of privacy in files that anyone who had access to the network could download. See id. at 1048. The court ruled this way notwithstanding the defendant's attempts to keep the files private because even though his subjective intent demonstrated a desire for privacy, it would be objectively unreasonable to uphold an expectation of privacy "in the face of such widespread public access." Id. The court also rejected the defendant's argument that the special forensic software used by investigators constituted a search. It cited several other cases supporting the proposition that special tools could be used to access already-public information, like the files in this case, because public information enjoys no Fourth Amendment protections. See id. at 1048.

- United States v. King, 509 F.3d 1338 (11th Cir. 2007). Defendant had child pornography on a personal computer connected to a military base network. Id. at 1339. His "files were 'shared' over

the entire base network," id. at 1342, and an airman searching the network remotely downloaded those files, id. at 1340–41. The defendant took several steps—ultimately unsuccessful—that he believed shielded his hard drive from access by others. Id. at 1341. Even though the defendant manifested a subjective expectation of privacy by attempting to secure the files, id., the court found that his failure to actually secure the files rendered that expectation objectively unreasonable, id. at 1342. In reaching this conclusion, the court analogized to a prior case holding that a defendant had no objectively reasonable expectation of privacy in the unsecured common area of a multi-unit apartment building. Id. In both cases, the fact of public access rendered any subjective expectation of privacy objectively unreasonable. Id.

- United States v. Ladeau, No. 09–40021–FDS, 2010 WL 1427523 (D. Mass. April 7, 2010). Defendant shared child pornography over a secured peer-to-peer network that allowed him to select who could download his files. Id. at *1. He allowed downloads by a private user who then turned his account over to the Royal Canadian Mounted Police. Id. The court held that even though the defendant manifested a subjective expectation of privacy through his actions, this expectation was not objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at *4. "No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access." Id. So, "[o]nce Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable." Id. at *5.

- United States v. Thomas, Nos. 5:12–cr–37, 5:12–cr–44, 5:12–cr–97, 2013 WL 6000484 (D. Vt. Nov. 8, 2013). Defendants in this case shared child pornography over peer-to-peer networks. Id. at *17. Police found the defendants by using automated scanning tools designed to detect child pornography shared on peer-to-peer networks. Id. After a lengthy explanation of file sharing, hash values, and investigative software and testing tools, id. at *2–6, the court held that the defendants had no reasonable expectation of privacy in files they shared publicly on a peer-to-peer network, id. at *19–20. In making this ruling, the court relied on United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010), along with other circuit cases. Id. at *19. The defendants argued against the inclusion of partially downloaded files in the evidence used against them, saying they would not have shared those files once the download was complete, but the court rejected this argument because those files were nonetheless being shared when the police searched and were therefore publicly accessible. Id. at *17. [Note: This case contains clear and thorough explanations of peer-to-peer networks, hash values, and TLO's CPS suite of tools.]

(6) Expectation of Privacy in Data That Is Not One's Own

The following cases address claims of a reasonable expectation of privacy in data that, in some sense, is not the movant's.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to

challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105,107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Almonor, the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Commonwealth v. Almonor, 482 Mass. 35, 47-48 (2019) (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The Court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Lugo, 482 Mass. at 108. During the investigation, police became concerned that a second juvenile involved in the murder-robbery might be in danger, and contacted that individual's cell phone service provider, obtaining location data, and the names and numbers from recent calls. Id. at 106. Among these was the defendant's phone number, which police also "pinged," showing that he was at his residence with the second juvenile. Id. Police obtained a search warrant for the residence and "discovered evidence linking the defendant to the killing, including the murder weapon." Id. The SJC pointed out that, even if there had been no standing issue, the circumstances of police investigating a homicide and concerned for the cell phone user's safety would have rendered the defendant's challenge futile under the emergency aid exception. Id. at 108. The Court also held that, while the defendant had standing to challenge the search of his own cell phone, the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 109.

- Commonwealth v. Bryant, 447 Mass. 494 (2006). Law enforcement seized the "main file server" of a law firm pursuant to a warrant. See Commonwealth's Brief, 2005 WL 4062684, at *10 (Dec. 2005). The defendant, an employee of the firm, moved to suppress files he had worked on. See Bryant, 447 Mass. at 495. Denying the motion to suppress, the Supreme Judicial Court held that the defendant did not have a "reasonable expectation of privacy" in the firm's files and therefore did "not establish[] that he ha[d] standing to challenge the seizure of the files." See id. at 497.

(7) Probationers, Parolees, and Court-Ordered Monitoring

Probationers subject to court-ordered monitoring have a diminished expectation of privacy.

- Commonwealth v. Feliz, 481 Mass. 689 (2019) (decided on the same day as Commonwealth v. Johnson, 481 Mass. 710 (2019), infra). The SJC held that Mass. Gen. Laws ch. 256, § 47, which mandates GPS monitoring as a condition of probation in connection with most sex offense convictions, is "overinclusive" because "GPS monitoring will not necessarily constitute a

reasonable search for all individuals convicted of a qualifying sex offense." Id. at *1; Mass. Gen. Laws ch. 256, § 47 (2018). The Court held that, under Article 14 of the Massachusetts Declaration of Rights, an individualized determination of reasonableness is required for any search that is "more than minimally invasive," and "GPS monitoring is not a minimally invasive search." 2019 WL at *7. Thus, a judge must "conduct a balancing test that weighs the Commonwealth's need to impose GPS monitoring against the privacy invasion occasioned by such monitoring." Id. at *1. Whether the monitoring is determined to be reasonable "depends on a constellation of factors," and "no one factor will be dispositive in every case." Id. at *8. The fact that a probationer accedes to a contract of probation that requires GPS monitoring or signs a GPS equipment contract does not constitute consent that waives the probationer's Article 14 rights. Id. at *8. With respect to Mr. Feliz, the SJC held that "the Commonwealth's particularized reasons for imposing GPS monitoring . . . do not outweigh the privacy intrusion occasioned by the requirement of GPS monitoring." Id. at *8; accord id. at *10–13. In support of that conclusion, the Court noted that the defendant "was convicted of noncontact sex offenses," and that the Commonwealth "ha[d] not presented evidence sufficient to indicate that th[e] defendant pose[d] a threat of reoffending or otherwise violating the terms of his probation." Id. at *10.

- Commonwealth v. Johnson, 481 Mass. 710 (2019) (decided on the same day as Commonwealth v. Feliz, supra). At defendant's trial for breaking and entering and larceny, the Commonwealth introduced GPS location data recorded from a GPS monitoring device that the defendant was wearing as a condition of probation. Id. at *1. The historical GPS data had been retrieved and reviewed without a warrant after the defendant's probation was completed. Id. at *2–3, *6. Defendant argued that the trial court erred in admitting the GPS location data at trial. Id. at *3. The SJC held that (1) the original imposition of GPS monitoring as a condition of defendant's probation was a search, but it was reasonable "in light of the defendant's extensive criminal history and willingness to recidivate while on probation"; and (2) no subsequent search occurred because, "once the GPS device was attached to the defendant, he did not possess a reasonable expectation of privacy in data targeted by police to determine his whereabouts at the times and locations of suspected criminal activity that occurred during the probationary period." Id. at *1. The SJC noted that the police had conducted a narrow analysis to determine whether the defendant was present at times and places where crimes had been committed, and that a broader "indiscriminate rummaging" through months of GPS data "might raise different, more difficult constitutional questions about objective expectations of privacy, even for a probationer subjected to GPS monitoring." Id. at *10.

- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017). Police investigating a robbery "mapped" the location of a defendant wearing a GPS monitoring device while out on bail for a domestic violence offense. See id. at 298. This process revealed that the defendant was near the scene of the robbery at the time of the break-in. See id. The Commonwealth introduced the GPS evidence at trial and the defendant was convicted. Id. at 296–97. The Massachusetts Appeals Court affirmed, rejecting defendant's argument that he—subject to court ordered monitoring—retained a reasonable expectation of privacy in his movements and thus was subject to a Fourth Amendment "search". See id. at 306.

Parolees have a diminished expectation of privacy—lower even than that of probationers—both under the Fourth Amendment, Samson v. California, 547 U.S. 843, 850 (2006), and under art. 14, Commonwealth v. Moore, 473 Mass. 481, 485 (2016). In Moore, the SJC determined that, "at least with respect to a search of the parolee's home," the reasonable suspicion standard associated with stop and frisk is the appropriate standard for a warrantless search. Id. at 487. Reasonable suspicion for the search of the home was supplied here by an anonymous tip that the parolee was dealing drugs, coupled with evidence of the parolee's conduct consistent with that tip in light of the parole officer's experience with narcotics and with other parolees. Id. at 490.

b) Seizures and Interference with Possessory Interest

Police actions reaching an individual's property constitute a seizure when "there is some meaningful interference with an individual's possessory interests in that property." Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (internal quotation marks omitted). As Justice Stevens noted in Texas v. Brown, 460 U.S. 730 (1983), "a seizure is usually preceded by a search, but when a container is involved the converse is often true . . . for example, the seizure of a locked suitcase does not necessarily compromise the secrecy of its contents . . . ." Id. at 747–48 (Stevens, J., concurring). Relying on ample precedent from other courts, the Supreme Judicial Court has found the entire computer analogous to such a closed container for seizure purposes. See Commonwealth v. McDermott, 448 Mass. 750, 766 (2007) (agreeing with lower-court "judge's analogy to closed containers with respect to the seizure of the computers and disks"). Whether a seizure has occurred is usually obvious and rarely contested. The following cases concern less-common circumstances.

- Berger v. New York, 388 U.S. 41 (1967). The Court held that wiretaps "seize" conversations in violation of the Fourth Amendment. Id. at 59. The Court did not expand further on how it came to this conclusion, but this case is often cited for the proposition that intangibles (e.g., data) can be seized in the constitutional sense. See, e.g., LeClair v. Hart, 800 F.2d 692, 695 (7th Cir. 1986) ("Following Berger, it has been clear that the Fourth Amendment embraces more than just the forced physical removal of tangible objects . . . . Indeed, Berger stands for the proposition that the government may seize intangible items, such as the information contained in the financial documents which the IRS agents copied.").

- Commonwealth v. Connolly, 454 Mass. 808 (2009). As part of an investigation of a suspected drug dealer, police installed a GPS tracking device in his car. Id. at 10. To install the device, police opened the car's engine compartment, placed the tracking device inside, and attached it to the car's battery. See id. at 812. The Supreme Judicial Court held that installing the GPS device was a seizure within the context of art. 14 of the Massachusetts Declaration of Rights. Id. at 822. First, the installation and presence of the tracker constituted a physical intrusion on the defendant's property. Id. Second, the government's use of the vehicle to obtain information was itself an interference with the defendant's interest in it. Id. at 823 ("It is a seizure not by virtue of the technology employed, but because the police use private property (the vehicle) to obtain information for their own purposes.").

- United States v. Hicks, 438 F. App'x 216 (4th Cir. 2011). Defendant destroyed his hard drive after he found out he was under investigation for possession of child pornography. Id. at 18. After he was convicted of destroying records in a federal investigation, the defendant attacked his conviction on constitutional grounds. Id. One of these challenges was that by criminalizing his destruction of his hard drive, the government had interfered with his possessory interest in that hard drive, effectively seizing it in violation of the Fourth Amendment. Id. at 219. The Fourth Circuit found that there was no meaningful interference with the defendant's possessory interest because he did not have a property right in images of child pornography. Id. (citing Helton v. Hunt, 330 F.3d 242, 247 (4th Cir. 2003), for the proposition that there is no property right in contraband).

The case summarized below discusses the return of unlawfully seized property:

- Commonwealth v. Salmons, 96 Mass. App. Ct. 61 (2019). The defendant pled guilty to assault and battery by means of a dangerous weapon, intimidating a witness, strangulation, and other charges. The police had seized the defendant's three cell phones at the time of arrest, but the seizure was subsequently found unlawful based on the SJC's decision in Commonwealth v. White, 475 Mass. 583 (2016) (probable cause to seize or search a cell phone requires "information establishing the existence of particularized evidence likely to be found there," id. at 593). Salmons, 96 Mass. App. Ct. at 62. The defendant filed a motion for the return of his cell phones, which was granted. Id. at 62. Eight months later, the Commonwealth moved to wipe the content of two of the phones before returning them, because they contained "numerous and sexually explicit photographs and videos of the defendant and [the victim]." Id. The motion to wipe these phones was allowed, id. at 65, but the Appeals Court reversed. Relying on Commonwealth v. Sacco, 401 Mass. 204 (1987), the Court found that "when, as here, property is unlawfully seized without a warrant, cannot be used as evidence, and is not unlawful to possess, it should be returned, upon proper motion, to its undisputed owner or the owner's representative." Salmons, 96 Mass. App. Ct. at 68. There was no factual finding that harm to the victim would occur unless the phones were wiped. Id. at 69. Further, the Commonwealth's reliance on Beldotti v. Commonwealth, 41 Mass. App. Ct. 185 (1997) was misplaced because the public interest standard of G.L. c. 276, § 3 did not apply to property seized unlawfully and because the "connection between the crime and the property here [was] far more attenuated than in [Beldotti]." Id. at 69-70.

c) Private Party Searches

(1) Initial Search Made by Private Party

"[W]hen the state conducts a search in response to information that a private party obtained and communicated to the government, 'the legality of the governmental search must be tested by the scope of the antecedent private search.'" Commonwealth v. Cormier, 28 Mass. L. Rptr. 489, at *4 (Mass. Super. Ct. 2011) (quoting United States v. Jacobsen, 466 U.S. 109, 116 (1984)). Where the government searches something in which a private party has already eroded a suspect's expectation of privacy, the Fourth Amendment is not implicated. Id. (citing Jacobsen, 466 U.S. at 116). Crucially, police examination of

materials "initially discovered and viewed by a private party" can be more thorough than that private party's examination and still fall within the scope of the private party search. Id. at *5 (citing Commonwealth v. Raboin, 24 Mass. L. Rptr. 278, 282–83 (Mass. Super. Ct. 2008)). A more detailed analysis of Commonwealth v. Cormier below demonstrates how the private party search doctrine applies to digital evidence cases.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. at *2. Police found more child pornography at the defendant's house, and he was later charged with possession. Id. The trial judge denied defendant's motion to suppress because the warrantless search conducted by police was within the scope of the preceding private party search. Id. at *4–6. Because the computer technician had previously viewed files from the hard drive, the court found that the defendant's expectation of privacy "had already been eroded," so the subsequent police search did not implicate the Fourth Amendment. Id. at *5.

(2) Warrantless Search: Private Citizen or State Actor

If the intent of a private party conducting a search is not independent of the government's intent, however, the private party becomes an agent of the government, implicating the Fourth Amendment and art. 14. See Commonwealth v. Leone, 386 Mass. 329, 333 (1982). A party becomes a state actor if the police do anything to "solicit, provoke, or tempt" that party into obtaining evidence for them. Commonwealth v. Brandwein, 435 Mass. 623, 631 (2002). The cases below examine the state actor issue in the digital evidence context.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. The court found that the data recovery shop employee was not acting as a state agent because he was a private party not acting under the authority of the state. Id. at *4 (citing Commonwealth v. Leone, 386 Mass. 329, 333 (1982), for the proposition that "[e]vidence discovered and seized by private parties is admissible without regard to the methods used, unless State officials have instigated or participated in the search"). The court noted that the employee "made the decision to open the suspicious files . . . as a private citizen, while trying to repair the hard drive at [defendant's] request." Id. The court also found that authorities "did not know that [the defendant] asked [the employee] to repair his hard drive and did not instruct [the employee] to inspect the files." Id. They did nothing "to 'solicit, provoke, or tempt' [the employee] into viewing the files," so he was not a state actor. Id. (quoting Brandwein, 435 Mass. at 631).

- United States v. Lichtenberger, 19 F. Supp. 3d 753 (N.D. Ohio 2014). A private party called police after discovering child pornography on a computer, and the responding officer instructed that individual to boot up the laptop, enter the password, show the images, and gather other devices belonging to the defendant before seeking a warrant. Id. at 754–55. The court found these actions violated the Fourth Amendment because by giving instructions and directing the private party's actions, the police officer made that private party into a government agent. Id. at 758–59. The court therefore suppressed the evidence as having been collected in violation of the Fourth Amendment. Id. at 760.

(3) An ISP's Reporting Obligation Does Not Make it a State Agent

The reporting requirement of 18 U.S.C. §§ 2258A(a) and 2258B(a)—requiring an Internet service provider (ISP) to report any child pornography that it discovers—does not transform an ISP into a government agent when it chooses, voluntarily, to scan files sent on its network for child pornography. United States v. Stevenson, 727 F.3d 826, 829–30 (8th Cir. 2013).

2. Was a Search or Seizure Reasonable?

"The ordinary rule is that to be reasonable under the [Fourth] Amendment a search [or seizure] must be authorized by warrant issued by a magistrate upon a showing of probable cause." Almeida-Sanchez v. United States, 413 U.S. 266, 287 (1973); see also United States v. Carpenter, 138 S. Ct. 2206, 2221 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.") (quoting Riley, 134 S. Ct. at 2482)). This section will lay out the requirements of a valid warrant in the cybercrime context and then highlight some applicable exceptions to the warrant requirement.

a) Warrants

"The Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights require that a warrant be issued only on probable cause, supported by oath or affirmation." Commonwealth v. Nelson, 460 Mass. 564, 568 (2011). Massachusetts law specifically "require[s] an affidavit and an oath." Id. (citing Mass. Gen. Laws ch. 276, §§ 1 and 2B). A neutral magistrate must issue the warrant, see Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971), and it must be particular as to the items to be seized and places to be searched, see Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Warrants must contain information that has not been rendered stale, see United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (to evaluate staleness, courts "must assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information"). In addition, officers must execute warrants in a timely fashion, see Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 329–30 (2014) ("[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event no later than seven days from the date of issuance thereof." (quoting Mass. Gen. Laws c. 276, § 3A)). Warrants must be executed in a reasonable manner. Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). Finally, executing officers must have the signed

warrant with them when commencing the search. The sections below focus on probable cause, particularity, staleness, timely execution, and the manner of executing warrants in the digital evidence context.

(1) Probable Cause / Affidavit

"Under the Fourth Amendment and art. 14, probable cause requires a substantial basis for concluding that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues." Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009) (internal quotation marks and citations omitted) (detailed below). Further:

> The affidavit need not convince the magistrate beyond a reasonable doubt, but must provide a substantial basis for concluding that evidence connected to the crime will be found on the specified premises. Moreover, affidavits for search warrants should be interpreted in a commonsense and realistic fashion and read as a whole, not parsed, severed, and subjected to hypercritical analysis. All reasonable inferences which may be drawn from the information in the affidavit may also be considered as to whether probable cause has been established.

Commonwealth v. Donahue, 430 Mass. 710, 712 (2000) (internal quotation marks and citations omitted).

In order to establish probable cause, law enforcement officials must typically submit an affidavit to a magistrate. That magistrate's probable cause determination is confined to the "four corners" of the affidavit. Commonwealth v. Anthony, 451 Mass. 59, 68 (2008) (detailed below). Probable cause by definition deals with "probabilities," which "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Id. (internal quotation marks and citations omitted). The following cases address probable cause and affidavits in the digital evidence context.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. The warrant affidavit "provided a substantial basis to conclude both that the defendant had committed the homicide [with a] coventurer and that it was reasonable to expect that his cell phone would contain evidence related to that specific crime." Id. at 587. Here, unlike in Commonwealth v. White, 475 Mass. 583 (2016), there was specific evidence of a nexus between the crime and the defendant's cell phone. Id. at 589. This evidence included the following facts: "the defendant made a cell phone call soon after the shooting to the person who rented the car used in the murder, there [was] a reasonable inference that the crime was

preplanned, and there [were] records of threatening cell phone communications between [the defendant's [coventurer] and the victim." Id.

- Commonwealth v. Vasquez, 482 Mass. 850 (2019). The defendant was indicted on charges of murder in the first degree and two related firearms offenses. He moved to suppress witnesses' identification of him from surveillance footage, his statements to the police, as well as evidence obtained from the search of his phone and the CSLI. Id. at 851. The SJC found that the witness identification did not require suppression. But the SJC agreed with the trial court's finding that the Miranda warnings were rendered in Spanish "in such a fragmented and confusing manner so as to be incoherent." Id. at 862. More specifically, the improper translation rendered the warnings "inadequate to apprise the defendant of his rights, and [ ] the defendant's limited comprehension of English did not suffice to compensate for these deficiencies." Id. at 852. Because the Miranda warnings were insufficient and the search of the defendant's cell phone arose from the statements the defendant made after the defective warnings, the search was not sufficiently attenuated from the unwarned statements. Id. at 865. Further, without the tainted information from the unwarned statements (such as the defendant's disclosure of his phone number), the Commonwealth failed to establish "the requisite nexus between the commission of [the] crime and the CSLI for the defendant's device." Id. at 867. The Commonwealth also failed to establish a connection between the crime and the thirty-two days for which it sought CSLI. Id. In sum, the search warrant affidavit did not "support a determination of probable cause, and the CSLI obtained as a result must be suppressed." Id. at 868. The SJC remarked in a footnote, however, that CSLI evidence may be admissible later, if the Commonwealth could show by a preponderance of the evidence that there was an untainted source for the nexus between the crime and CSLI. Id. at 868 n. 27 (quoting Commonwealth v. Estabrook, 472 Mass. 852, 865 (2015)).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). Following conviction for first-degree murder, the defendant argued on appeal, among other things, that the motion judge erred in denying his pre-trial motion to suppress cell site location information (CSLI) that was introduced as evidence during his trial. Id. at 539. The defendant's brother had identified the defendant as the man leaving the crime scene in video footage, and provided police with a phone number he claimed belonged to the defendant. Id. at 541. Police then requested a court order requiring the service provider to produce CSLI from the cell phone for several months surrounding the day of the crime. Id. at 541. The CSLI placed the owner of the cell phone in the general vicinity of the crime at the time of the killing. Id. The Court ruled that, although it was a close call, the police affidavit in support of a search warrant for historical CSLI satisfied the requirement that "there be a substantial basis to believe that the sought-after CSLI 'will produce evidence of [the] offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed . . . such offense.'" Id. at 545-46 (quoting Commonwealth v. Augustine, 472 Mass. 448, 453 (2015)). The Court rejected the defendant's assertion that the police must demonstrate that the cell phone was used or possessed during the commission of a crime in order to show nexus between "the crime . . . the items sought, and the location to be searched." Id. at 546. This is not necessary because "[c]ell phones physically accompany their users everywhere such that tracking a cell phone results in near perfect surveillance of its user." Id. at 547 (quoting

Commonwealth v. Almonor, 482 Mass. 35, 45 (2019) (internal quotation marks omitted)). The defendant's brother's statement that the cell phone belonged to the defendant, together with subsequent corroboration by the defendant's former girlfriend, was enough to establish the requisite nexus. Id. at 548-49.

- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019). The indictments in this case alleged that the defendant and two co-conspirators broke into the defendant's uncle's home and beat him on the head and face with a crowbar. Id. at 618. The defendant was charged with home invasion, assault, and multiple other offenses. Id. at 618, n. 1. She moved to suppress the fruits of a search of her cell phone. The Superior Court allowed the motion, but the Appeals Court reversed, finding that the police had probable cause to seize the phone, and that the defendant voluntarily consented to an unlimited search of her phone. There was probable cause to seize the cell phone because the defendant told the police it contained videos that "could establish where, when, and with whom the defendant was in the hours before the home invasion." Id. at 623. The police were also aware of multiple facts connecting the defendant to the crime. For example, her car was seen near the victim's home less than two hours before the assault, she had a key to the victim's residence and there was no sign of forced entry, the victim had a restraining order against the defendant, and there were blood stains in the exterior of the defendant's car. Id. In sum, the seizure was lawful because the police had "a substantial basis for concluding" that the phone contained "evidence connected to the crime under investigation." Id. The court also ruled that the defendant's subsequent "consent to search her cell phone was without limitation." Id. at 625-26. The police communicated their intent to search the entire cell phone to the defendant, and she consented to the search, providing the police with passwords to the phone and to her Snapchat account. Id. at 626. Applying "a common sense interpretation" to the defendant's entire exchange with the police detective, the Appeals Court found that her "consent to search her cell phone was free, voluntary, and unlimited." Id.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police approached the defendant sleeping in the stairwell and seized a cell phone on the floor nearby. Id. at 282. There was probable cause to seize the phone because the police "had information that the defendant and victim had been together on the day of the murder, and also that [the murder victim's boyfriend] had recently overheard the defendant confessing to the murder to an unidentified person on a cell phone." Id.

- Commonwealth v. Martinez, 476 Mass. 410 (2017). State police used law enforcement version of P2P client to investigate sharing of child pornography, identified such activity coming from a Massachusetts IP address, and subpoenaed Comcast for information regarding the IP address for the 30-minute period on March 9, 2012, during which police downloaded four suspected child pornography video files shared from the account associated with the IP address. Id. at 411–13. The ISP gave police a name (Angel Martinez) and an address. Id. at 413. Local law enforcement then obtained a warrant to search the apartment located at the address for computers and related items connected to the suspected possession and distribution of child pornography. Id. The apartment was leased to the grandmother of the Comcast account holder and of the defendant (Adalberto Martinez). Id. at 413 n.2. Law enforcement seized two laptops belonging to the

defendant and found five videos containing child pornography on one of them. Id. The SJC held that the affidavit in support of the search warrant (containing information that a particular IP address was used to share child pornography and that this IP address had been assigned at the time to a subscriber at the specific physical address to be searched) was sufficient to establish probable cause for the search, even though the named subscriber was neither listed as, nor confirmed to be, living in the apartment searched, and even though police had no information before the search linking the defendant to the residence. According to the SJC, law enforcement did not have to verify that the account holder lived at the address searched. Id. at 418. Once the nexus between the crime and the service address was established, the names of the account holder and of the leaseholder were incidental. Id. The SJC rejected the argument that law enforcement had to show that the network was secure or that no one outside the address could access the network. Id. at 419. Where the warrant was for the search of a place (not for the arrest of a person), law enforcement needed only demonstrate a sufficient nexus between the criminal activity under investigation, the items sought, and a place to be searched. Id. Even assuming law enforcement could know a network was not secured, unauthorized use of the network did not negate the substantial basis to think the evidence would be located at the address. Id. at 420–21 ("[P]robable cause does not require investigators to 'establish to a certainty that the items to be seized will be found in the specified location,' nor does it require them to 'exclude any and all possibility that the items might be found elsewhere.'" (quoting Anthony, 451 Mass. at 70)).

The decision came with caveats. The SJC cautioned that its decision here does not mean that probable cause always exists any time investigators link illegal computer activity to an IP address and then link that IP address to a physical address. Martinez, 476 Mass. at 422. To support probable cause, law enforcement should use reliable methods—such as the administrative subpoena here—to connect the IP with a physical address, not IP address mapping services. Id. at 423. Additionally, some technologies (e.g., Tor exit relays, VPNs, and proxy server connections, which can mask originating IP addresses) may erode the connection between an IP and a physical address. Id. Law enforcement may be required to disclose in affidavits the possibility that one of these technologies was, or may have been, used based on facts known or reasonably knowable to investigators at the time. Id. "If such technologies become more common, it is entirely possible that we would require police to proceed in multiple steps, obtaining subpoenas related to each intermediary IP address or warrants to search each location hosting those IP addresses." Id. In some cases, law enforcement may be required to determine, by forensic examination of a wireless router, which devices were connected to it and when before searching particular computers. Id.

- Commonwealth v. Perkins, 478 Mass. 97 (2017). "Based on intercepted telephone conversations between defendant's alleged middleman and street-level distributor of cocaine, police surveillance of suspected drug transaction, and other information, the judge issued a warrant authorizing a search of the defendant's apartment for evidence including a cellular telephone and drug-related records." Id. at 99. The warrant also included authorization to seize currency, distribution paraphernalia, documentation about the premises and its contents, among other items. Id. at 101. The affidavit did not seek authorization to search for narcotics. Id. at 98. Police seized a large quantity of cocaine, several cell phones, drug paraphernalia, and ammunition. Id. at 101.

The SJC concluded that the affidavit justified searching the apartment for the defendant's phone. Id. at 105–06. They further concluded that the seizure of nine additional phones found in the apartment was supported by probable cause, but that the police did not have discretion to "search every portion" of these additional phones. Id. At 106. Instead, the plain terms of the warrant restricted their search to call activity and contact lists and did not authorize police to "rummage through the entirety of the defendant's cellular telephones." *Id*. At 106. With regards to searching the defendant's apartment for records, proceeds, and paraphernalia, however, the SJC held that the affidavit:

> did not contain sufficient particularized information to justify [such] a search of the defendant[']s apartment . . . . The affidavit included a single, conclusory statement that probable cause existed based on the affiant's "training and experience and the facts and circumstances learned during the course of this investigation," [but] contained no facts, or opinion based upon the affiant's considerable experience as a narcotics officer, that would have establish[ed] probable cause to believe that the defendant would be likely to store particular items of [drug-related records, proceeds, or paraphernalia] in his home.

Id. at 109.

- Commonwealth v. Jordan, 91 Mass. App. Ct. 743 (2017). In a murder investigation in which defendant was a suspect, police obtained search warrant for his CSLI, call details, text messages, and subscriber information for a six-week period surrounding the date of the homicide. Id. at 744. The Appeals Court found that the trial judge properly suppressed the text messages. Id. Although the affidavit in support of the warrant established probable cause to believe that the victim had been murdered (i.e., a crime had been committed), it made no connection between the defendant's use of his cell phone and his involvement in the crime, and thus did not establish probable cause to conclude that the text messages would provide evidence connected to the crime. Id. at 749–51. The affidavit did establish probable cause to conclude that the defendant committed the crime and showed that the defendant had a cell phone and that it was in use around the time of the murder, and so it established probable cause to believe that the CSLI would provide evidence of the defendant's involvement in the crime. Id. at 750–53. The SJC also held that the trial court had properly suppressed "contact information" insofar as that meant an address book or contact list because the affidavit failed to establish a nexus between the crime and the defendant's contact information. Id. at 753–54. However, if "contact information" meant subscriber information and call records, there was no basis for suppression. Id.

- Commonwealth v. Keown, 478 Mass. 232 (2017). Defendant was suspected of murdering his wife by poisoning her. In the course of the investigation, police obtained a warrant to search his computer and discovered evidence of incriminating Internet searches, which was introduced at trial. Id. at 234–37. The SJC held the affidavit established a sufficient nexus between the crime and the item sought where: (1) it established the defendant's sophistication with computers (he had worked as a Web designer), and showed that he had forged contracts and admissions letter/other communications from Harvard Business School (can infer he used computer); (2) it described forgeries related to the motive alleged in the affidavit, i.e., to kill his wife to prevent her

finding out about their impending financial ruin and his lies and to collect her life insurance benefits; (3) it specified that the victim had died from ethylene glycol poisoning which, the affiant noted, would likely have involved online research. Id. at 238–39.

- Commonwealth v. Broom, 474 Mass. 486 (2016). At the time of defendant's arrest for murder, his cell phone was seized. Id. at 494. Ten months later, law enforcement applied for and obtained a search warrant for its contents. Id. The affidavit contained information about the investigation and the fact that no CSLI information could be obtained for the time surrounding the murder but that the defendant's phone records showed he sent and received text messages and accessed the Internet at the relevant timeframe. Id. It then described the many types of data the detective wanted to search in order to uncover information pertinent to the investigation. Id. at 494–95. The SJC held the search was not supported by probable cause. Id. The Court held that "it is not enough that the object of the search *may* be found in the place subject to search. Rather, the affidavit must demonstrate that there is a reasonable expectation that the items sought *will* be located in the particular data file or other specifically identified electronic location that is to be searched." Id. at 496 (citations omitted) (emphasis in original). Police here already had the defendant's CSLI (except for the time period surrounding the murder) and call records and would have known that the victim's number did not appear in those records. Id. The warrant was also found to be too broad. Id. at 495, 496 n.13.

- Commonwealth v. White, 475 Mass. 583 (2016). A police investigation of an armed robbery and shooting led to the defendant as one of three suspects. Id. at 584. After suspicion focused on him, the detective located his phone, which was held by the defendant's school administrator pursuant to school policy. Id. The detective then "seized the telephone to prevent the defendant from retrieving it and removing evidence or destroying the device." Id. Police had no information at the time indicating that the phone had been used to plan, commit, or cover up the armed robbery they were investigating, or that it contained any evidence of the crime, but instead relied on knowledge that cell phones are frequently used when the offense involves multiple perpetrators. Id. Sixty-eight days after the seizure, police obtained a warrant to search the cell phone and found evidence that was later ordered suppressed. Id. The SJC held that the seizure was not supported by probable cause because probable cause may not be based solely on an officer's opinion that the device is likely to contain evidence of the crime under investigation. Id. at 584–85. "[E]ven where there is probable cause to suspect the defendant of a crime, police may not seize or search his or her cellular telephone to look for evidence unless they have information establishing the existence of particularized evidence likely to be found there." Id. at 590–91. A contrary decision would mean that, where probable cause to charge someone with a crime existed, the person's phone would almost always be subject to seizure and subsequent search. Id. at 591.

- Commonwealth v. Williams, 90 Mass. App. Ct. 1118 (2016) (unpublished). The victim was shot after a drug deal with two suspects. Id. at *1–2. Two witnesses testified that the victim had arranged the deal via phone. Id. Police zeroed in on an 857 (area code) number linked to a person named Patrick Malone. Id. Defendant was then identified as the second suspect and was interviewed by police; he stated that he had known Malone for twenty years and that they had a

phone conversation on the morning of the shooting. Id. at *3–4. Police seized the defendant's iPhone and secured it to get a warrant. Id. The Appeals Court held that "there was probable cause to believe that the defendant's iPhone would contain evidence linking his alleged coventurer Malone to the 857 number and thus to the shooting." Id. at *5. See also Commonwealth v. Perkins, 478 Mass. 97, 105–06 (2017), (where police had detailed and specific knowledge about the defendant's use of a cell phone to arrange drug transactions, and a particular phone number with which that cell phone had been in contact at a specific time, there was probable cause to believe that the defendant used a cell phone to arrange a drug sale and that he had done so on other occasions and the seizure of nine cell phones from his apartment was proper). But see Commonwealth v. Fulgiam, 477 Mass. 20, 34 (2017) (where warrant application established a personal relationship between defendant and victim and the circumstances of the murders suggested a connection to drugs, it did not, without more, justify intrusion into the content of the communications between defendant and victim).

- Commonwealth v. Finglas, 81 Mass. App. Ct. 1102 (2011) (unpublished). Police were sent information about the defendant, whose email address had received five images depicting child pornography. Id. at *1–2. On interlocutory appeal, the Appeals Court granted the defendant's motion to suppress evidence obtained as a result of a search of his residence. Id. at *3. It did so because the affidavit in support of the warrant was "inadequate to establish a timely nexus between the defendant and the location to be searched and to permit the determination that the particular items of criminal activity sought reasonably could be expected to be found there." Id. The Appeals Court held that the affidavit did not provide any evidence that a computer at the residence had been used to search for or download any child pornography or that the defendant had actually accessed the emailed images. Id. at *2. Further, a police officer's opinion about the common practices of child pornography collectors was not enough, without further facts, to support a finding that the defendant's computer likely contained child pornography. Id. at 3.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it based on an affidavit alleging: (1) both shared folders had a copy of the same pirated movie, (2) the second computer's shared folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 105, 107–09. The Court invalidated the search warrant because it found police did not provide a "substantial basis" to believe there would be child pornography on the computer. Id. at 111. The Court found it unreasonable to infer that somebody interested in sharing a commercial movie would also be interested in sharing child pornography. Id. at 112. That the defendant had access to child pornography did not help the Commonwealth's case. Id. Nor was a suspicious statement, standing alone, enough to provide the substantial basis necessary for probable cause. Id. at 113.

- Commonwealth v. Anthony, 451 Mass. 59 (2008). Police received a tip about a person soliciting child pornography online. Id. at 60–62. They traced these solicitations to a library and arrested a

homeless suspect there. Id. at 62–63. Shortly after the arrest, the suspect took a receipt (along with other pieces of paper) out of his pocket and tore it up. Id. at 63. This receipt was from a repair shop for the repair of two laptops. Id. Police also determined he rented a storage locker. Id. at 64. Police sought and received a search warrant for the locker, the laptops, and a hard drive from the library. Id. at 65–66. A superior court judge granted the defendant's motion to suppress for lack of probable cause, however, and the Commonwealth pursued an interlocutory appeal. Id. at 67–68. The SJC reversed the motion judge's suppression of the warrant, finding the affidavit established probable cause. Id. at 73. Specifically, the Court found information about the suspect's prior conviction for child pornography, the outside tip, and the suspect's admission to viewing child pornography in violation of his probation established probable cause for the crime. Id. at 70–71. From there, it found the fact that a homeless individual rented a storage locker using a false address—along with the detective's experience that viewers of child pornography tend to collect it—supported the idea that the suspect might hide child pornography at his storage locker, the only space under his control. Id. at 71–72. The Court found the suspect tearing up the receipt supported the inference that he was trying to hide child pornography. Id. at 71. It emphasized that the affidavit did not rely solely on the opinions of the affiant with respect to general characteristics of collectors of child pornography. Id. at 72. Rather, the affidavit contained enough facts and inferences to support a nexus between the alleged crime and the locations to be searched. Id. 72–73.

(2) Independent Source Doctrine

- Commonwealth v. Wilson, 486 Mass. 328 (2020). The police initially obtained defendant's CSLI data pursuant to an § 2703 order, without a warrant, in 2010. Id. at 336. The CSLI placed the defendant in "the victim's hotel, at the commuter lot where the [victim's] rental vehicle was found, and in the location where the victim's body would later be discovered, at relevant times on the night of the murder." Id. at 331. In 2014, the police obtained the same CSLI information pursuant to a search warrant. The Court found that the 2014 warrant satisfied the "independent source doctrine," "a well-recognized exception to the exclusionary rule under both the Fourth Amendment and art. 14." Id. at 335. The doctrine provides that "evidence initially discovered as a consequence of an unlawful search may be admissible if later acquired independently by lawful means untainted by the initial illegality." Id. (quoting Commonwealth v. DeJesus, 439 Mass. 616, 624 (2003)). Here, the affidavit supporting the 2014 warrant for the CSLI was based on facts wholly independent of the CSLI data obtained in 2010. Id. at 336. These facts included the following: the defendant's public statements about having a firearm like the one used in the murder, his status as the likely father of the victim's unborn child, causing financial obligations to the victim and the "ire of the defendant's wife," the victim's statement to a friend that the defendant asked her to get an abortion, the cellphone communications between the defendant and the victim until shortly before the victim's cellphone activity ceased at 10:49 P.M. on the night of the murder, and a Facebook message from the victim's account after she was reported missing "claiming she was in the hospital after an abortion, although police determined that she was not a patient at any area hospitals." Id. at 337.

- Commonwealth v. Gosselin, 486 Mass. 256 (2020). The defendant appealed his conviction for first-degree murder, arguing, *inter alia*, that his trial counsel was ineffective for not moving to

suppress CSLI evidence, as such evidence provided probable cause for the search warrant for his home—the search of which produced critical inculpatory evidence. Id. at 264. The Court declined to resolve whether the § 2703 warrant was supported by probable cause, on the grounds that "the search warrant affidavit satisfied probable cause when excising the unconstitutionally obtained CSLI," such that the defendant failed to demonstrate prejudice and his trial counsel was not ineffective. Id. at 264-66 & n.9.

(3) Particularity / Scope

The Fourth Amendment, art. 14, and Mass. Gen. Laws ch. 276, § 2 all require that search warrant applications particularly describe the places to be searched and the items to be seized. See Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Massachusetts courts treat these provisions as coextensive. Id. The dual purpose of these requirements is (1) to protect people from general searches and (2) to provide the Commonwealth the opportunity to demonstrate to a court that officers' search authorization was properly limited. Id. Additionally, the requirement provides essential information to a person whose property is being searched. Id. (citing Katz v. United States, 389 U.S. 347, 356 (1967)). The cases below explore the tension between the particularity requirement and the amorphous nature of data in the digital era.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. However, the Court concluded "that the search of the phone was not sufficiently particular because it lacked any temporal limit." Id. at 583. More specifically, the Court held "that (1) the correct remedy for the warrant lacking particularity in this case [was] partial suppression; (2) the search of text messages, call logs, and Snapchat video recordings was proper; yet (3) the lack of time restriction rendered the warrant impermissibly broad." Id. at 590. Accordingly, the SJC remanded the case to the Superior Court to determine whether "the proffered evidence fell outside what would have been a reasonable temporal limit." Id. First, as to partial suppression, the Court noted "that an overbroad warrant generally requires only partial suppression of the information for which there was not the requisite nexus, as long as the Commonwealth had not relied on or otherwise exploited it at trial. Id. at 591-92 (quotations and citations omitted). Second, because the police here had probable cause to search the defendant's cell phone for evidence of joint venture, the scope of the search properly included communications such as call logs, text messages, and Snapchat videos. Id. at 593. Third, a cell phone search warrant cannot be sufficiently particular without some temporal restriction that should "err on the side of narrowness." Id. at 594. Where the initial search provides probable cause to broaden the search, "nothing precludes" officers from requesting another, broader warrant. Id.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case involving partial suppression of CSLI, the government requested 48 hours of a shooting suspect's CSLI around the time of the shooting, received 34 hours of CSLI in response to this request, and then had all but

three hours of CSLI ("covering the period approximately ninety minutes before and ninety minutes after the shooting") suppressed by the trial judge. Id. at 164. The SJC upheld this partial suppression of CSLI data, but noted in dicta that the "severance doctrine [of Hobbs] is not without limits," and that "where a warrant so lacks particularity or is so overbroad that it begins to resemble a general warrant, total suppression is required." Id. at 168-69. The court deemed the CSLI request at issue "not so overbroad on the facts of this case so as to be akin to a general warrant" and found it to "represent 'a reasonable period of time encompassing the commission of and flight from the crime.'" Id. at 169 (quoting Hobbs, 482 Mass. at 550). However, the SJC declined to provide further guidance on exactly "how overbroad a request for CSLI must be in order for total suppression to be appropriate." Id.

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). The government requested three and a half months of historical CSLI from defendant's cell service provider, from December 1, 2010 to March 15, 2011, where defendant was a suspect in a December 16, 2010 killing. Id. at 543, 550. "This extended request was in part the result of the failure to identify the defendant as a suspect for nearly two and one-half months, and the absence of any evidence of his current location once he was identified as a suspect." Id. at 550. The SJC considered the question of whether "either the Fourth Amendment or art. 14 require[s] total suppression of the entire amount of CSLI collected," or whether "the proper remedy [is] to suppress only the CSLI for which there is not the requisite nexus to the crime," and concluded that "where the requisite nexus for probable cause clearly exists for a reasonable period of time" contained within the requested period, "the CSLI for [the relevant] period of time need not be suppressed so long as the CSLI for which there is not the requisite nexus to the crime is not relied on or otherwise exploited by the Commonwealth at trial." Id. However, the court suggested its holding was fairly narrow, noting that "[g]iven the uncertainty in the case law regarding overbroad requests for CSLI, we proceed cautiously on this issue." Id. The Court also "emphasized the significant constitutional issues raised by the collection of extended amounts of historical CSLI, and the importance of limiting the requests accordingly." Id. at 550 n.13.

- Commonwealth v. Holley, 478 Mass. 508 (2017). In a murder investigation, law enforcement examined the victim's call records and learned that the last call the victim answered before the shooting came from the defendant's telephone number. Id. at 511. Law enforcement then obtained cell phone records through a warrant served on the carrier and found multiple incriminating communications via text and call between the victim and the defendant's joint venturer. Id. The warrant for the phone records sought "subscriber information; billing records and detailed airtime; outbound call detail; call origination and termination location; stored GPS location information, and/or stored cellular tower records, cell tower sector information, range from cell tower information (RTT) and physical address of cell sites; and all stored contents of electronic or wire communications including stored or deleted voicemail, read, unread, deleted, or sent electronic mail or text messages, and stored files; and listing of all associated phone numbers, of a subscriber to or customer of such service" between October 1 and 18, 2012. Id. at 524–25. The broad scope of the search raised "significant concerns" for the SJC because it did not sufficiently limit the scope of the search so as to prevent "exploratory rummaging." Id. at 525,

528. But because the record was silent on how the provider conducted the search and on what information, if any, it provided to the Commonwealth beyond the text messages (it was even unclear whether the provider kept any stored content apart from text messages as part of its business records) and because the only communications used at trial were the defendants' redacted text messages from four and two days before the shooting, respectively, the day of the shooting, and the day after the shooting, the Court could find no error in the denial of the motions to suppress. Id. at 525 (noting that the "Commonwealth did not capitalize on the lack of particularity in the warrant").

- Commonwealth v. Molina, 476 Mass. 388 (2017). Police investigating a P2P network found child pornography shared by a Massachusetts IP address. They subpoenaed Verizon and obtained a name (Hermes Delcid) and service address. Id. at 390–91. Further investigation found the name on the mailbox outside of the address and RMV records showed Delcid at the address. Id. at 391. Police then obtained a search warrant for the apartment and in particular for electronic devices containing evidence of child pornography, evidence of child pornography in other formats, evidence related to access to the Verizon account and the P2P network, and evidence related to access to electronic devices at the apartment. Id. In a bedroom later identified as the defendant's, police observed the P2P program running on an open laptop (computer screen showed downloads and uploads of child pornography files in progress). Id. at 392. The search team seized numerous electronic devices from the apartment, including the defendant's laptop and desktop computers and his external hard drive. Id. On appeal, the defendant argued that the search warrant was impermissibly overbroad as to both places and "things" to be searched. Id. at 393. The SJC disagreed. Id. at 389. It found that the warrant appropriately substantiated a connection between the apartment and the evidence of child pornography reasonably expected to be located therein. Id. at 394. That the apartment was shared by multiple people was immaterial because the warrant authorized a search of the location associated with the IP address, not a search of any single associated subscriber. Id. at 395. Computer devices using the monitored IP could have been anywhere in the apartment, so where the defendant's unlocked bedroom showed no indicia of separate ownership from the rest of the apartment, the search of his bedroom was proper. Id. at 396. With regard to the things to be searched, the SJC made the following finding: "Because that evidence, in the form of electronic files, could be easily transferred between devices at the same location, police need not have limited the devices to be searched. Id. at 396. The SJC raised the reasonableness of the search *sua sponte*. Id. at 397. It found that where "multiple electronic devices that may well belong to multiple individuals are seized and searched, the reasonableness of the undertaking will be judged, at least in part, by whether the searches of those devices are conducted in a manner that seeks to limit the scope of the search as much as practicable in the particular circumstances." Id. at 397–98. The SJC may in the future "consider whether to require, as some courts have, a digital search protocol that would affirmatively demonstrate 'a high regard for rights of privacy and take all measures reasonable to avoid unnecessary intrusion.'" Id. at 398 (quoting Commonwealth v. Vitello, 367 Mass. 224, 262 (1975)).

- Commonwealth v. Keown, 478 Mass. 232 (2017). "The scope of the search authorized by the warrant included files on the laptop related to the health or death of the victim; other prominent

poisoning cases; ethylene glycol or other poisons; and the financial records, life insurance plans, and wills of the victim and the defendant." Id. at 240. The affidavit "established probable cause to search for evidence on the laptop computer relating to the defendant's role in his wife's death." Id. "These categories of evidence were related to the means of committing the crime and the motive of the defendant, and provided sufficient guidance to the examiners so that they were not on a fishing expedition." Id. In addition, the search was conducted reasonably. Id. at 241. Examiners used a list of 50 search terms that was later supplemented by 19 additional terms. While not part of the warrant application, the terms were related to the categories of evidence sought in the affidavit. "[T]he examiner only looked closely at approximately 325 files of the nearly 400,000 found on the laptop computer." Id. The search in this case "took place more than a decade ago in an entirely different technological landscape"; thus, the absence of an ex ante search protocol did not defeat particularity. Id. at 41.

- Commonwealth v. Dorelas, 473 Mass. 496 (2016). The defendant, who was a suspect in an assault and battery by means of a dangerous weapon (firearm) and an assault with intent to murder, was involved in a shooting. Id. at 497. Interviews with his family and friends indicated that prior to the shooting he had received threatening calls and texts. Id. at 498. Police believed the defendant's iPhone contained evidence linking the defendant and the other shooter to the assaults and obtained a warrant authorizing a search for, among other things, saved and deleted photographs. Id. at 498–99. The search resulted in the discovery and seizure of incriminating photographs. Id. at 499. The defendant contended that police only had probable cause for his call logs and text messages, but not his photographs. Id. at 500. On direct appellate review, the SJC reached the following holding: "Communications can come in many forms including photographic, which the defendant freely admits. So long as such evidence may reasonably be found in the file containing the defendant's photographs, that file may be searched." Id. at 503. Therefore, such a search is "neither outside the scope of the warrant nor unreasonable." Id. The defendant further argued that a search using the Universal Forensic Extraction Device (UFED) could have been conducted for communications, including photographic communications, without reviewing his photograph file. Id. at 504. The SJC held that such a retrieval method was not constitutionally required where the photographic evidence would also reasonably be found in the phone's photograph file. Id. The Court was concerned that texts and their attachments might be overwritten over time and the evidence would thus only be found in the photograph file. Id.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the shooting. Id. at 764–65. They seized five computers and disks. Id. at 765. The defendant asserted that this was unlawful because the warrant did not specifically authorize the seizure of these items. Id. at 770. The warrant did authorize, however, seizure of several types of documents. Id. at 771. The Court held that the seizure of the computers was reasonable because they functioned as "closed containers" storing documents. Id. at 766, 771. [Note: In Preventative Medicine Assocs. v. Commonwealth, 465 Mass. 810 (2013), the SJC clarified that in McDermott, the fact that the warrant was issued before an indictment as part of an investigation and the Commonwealth's use of preset search terms during the preliminary review of the defendant's

files were important to its holding, id. at 830–32. The Court stated that it took "seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained." Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.]

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. 2001). Police received information that defendant was distributing child pornography over the Internet. Id. at *1. They obtained a warrant allowing them to seize the defendant's computers and associated storage devices, to bring those items to a search location, and to search them for "visual images depicting children in a state of nudity or sexual conduct." Id. at *8. The defendant challenged the warrant as not particular enough because it allowed for seizure and search of all files on the computer, many of which were not related to child pornography. Id. The court denied the defendant's motion, noting that "where the commingling of legitimate and illegitimate items makes an on-site examination impracticable, a temporary seizure of the whole is permitted." Id. (citing various federal cases to that effect). It noted that "[t]he investigators could not have known in what form—whether on the computer hard drive or other various storage devices—the defendant was storing the target images. To insulate such images from search and seizure merely because other, non-incriminating items may have sheltered the images would pervert the accepted purpose of the constitutional bar against general searches." Id. at *9.

- United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013). Police received a tip that a Washington resident was sharing child pornography over a peer-to-peer networking site. Id. at 1043. They prepared a search warrant affidavit setting forth the information they had received about the suspect's IP address, the pornography he shared, general peer-to-peer network operations, data storage, and known characteristics of child pornography offenders. See id. The magistrate granted the warrant, which authorized seizure of all of the defendant's computers and data storage devices, and police discovered large quantities of child pornography. Id. at 1043–44. The trial judge suppressed the evidence reasoning that the warrant was facially overbroad. Id. at 1045. The Ninth Circuit reversed this decision. Id. at 1046. It based this ruling on the "practical, common-sense decision" judges make in issuing warrants. Id. at 1046. Specifically, the Ninth Circuit found that "[t]he government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files" and reasoned that "[t]he government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner." Id. Given this reasoning and supportive precedent, the court found the warrant permissible. Id. at 1047.

- In re a Warrant for All Content & Other Info. Associated with Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386

(S.D.N.Y. 2014). Federal agents investigating illegal money remitting applied for a search warrant to access a suspect's entire email account in search of specified emails. Id. at 388. The Magistrate considered and rejected the reasoning that such a search was akin to a general warrant and therefore failed the Fourth Amendment's particularity requirement. Id. at 390–91. First, the judge noted that extensive authority supported the proposition that investigators could briefly examine a wide variety of documents during a search in order to determine relevance. Id. at 391–92. Though that examination is essentially a seizure, it is also a practical necessity to determine which documents can be more permanently seized. Id. at 392–93. Next, he noted that courts have been more flexible with searches and seizures of electronic evidence because the large mass of undifferentiated information makes an on-site search impossible. Id. at 392. Courts have recognized the practical necessity of copying hard drives for later examination, allowing the government to access electronic information outside the scope of its search in order to effectuate that search. Id. at 393. Finally, the judge found that email provider employees would not be capable of performing the search themselves because they would not know enough about the investigation in order to properly recognize relevant emails. Id. at 395.

(4) Staleness of Information Supporting Probable Cause

In order to provide probable cause sufficient for a search warrant, the information contained in an affidavit supporting such a warrant must be sufficiently fresh. See United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (detailed below). In assessing staleness, courts "do not measure the timeliness of information simply by counting the number of days that have elapsed" but rather "assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." Id. (citing United States v. Pierre, 484 F.3d 75, 83 (1st Cir. 2007)). This requirement should not be confused with the separate Massachusetts statutory requirement (examined next) that warrants be timely executed after they have been issued. The following cases address staleness in the digital evidence context.

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that affidavit in support of the warrant to search his home did not establish probable cause because it was based on stale information: namely, an image depicting child pornography that was uploaded from the defendant's computer to the Skype service seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time (id. at 29), the Court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the Court identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a

single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]" – an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020). Defendant was convicted of unlicensed carrying of a firearm outside his residence or place of business. Id. at 420–21.The police obtained a search warrant based an affidavit that described (1) a series of images and videos of the defendant and an acquaintance handling a TEC-9 firearm at the acquaintance's house, which the two of them posted on Snapchat, and (2) location data from a GPS device that the acquaintance, Santos, who was subject to GPS monitoring, was wearing at the time of the Snapchat posts. Id. The defendant argued that because "Snapchat videos and images that are posted on a particular date may have been taken, created, or recorded at an earlier date and uploaded much later… the Commonwealth failed to prove that the information officers relied on from the timestamps on the defendant's and Santos's Snapchat uploads was not stale." Id. at 424. The court rejected the defendant's arguments on staleness, finding probable cause was established by a Snapchat post by Santos from two days before the search warrant was obtained and executed: an image of a TEC-9 (semiautomatic) firearm captioned "Shyt change on my block trust issues I got put all my trust in semi autos." Id. at 421, 424. The court characterized the caption as "a present tense statement about Santos's perceived need for semiautomatic weaponry[, g]iven [which] there was probable cause to believe that the Snapchat image was taken contemporaneously with its posting" (which, in turn, was only two days before the warrant was executed). Id. at 424. The court did not discuss whether, or under what circumstances, similar posts absent such a present-tense caption could have sufficed to establish probable cause.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police waited ten days to apply for a search warrant on a seized phone. See id. at 283. This delay was permissible because "the defendant's minimal possessory interest was far outweighed by the government's interest in obtaining evidence regarding a recent murder." Id.

- United States v. Morales-Aldahondo, 524 F.3d 115 (1st Cir. 2008). Defendant was convicted of possessing child pornography as a result of an investigation targeting a child pornography website and its subscribers. Id. at 117–18. The download information obtained from the website was over three years old by the time the search warrant in this case was issued. Id. at 119. On appeal, the court upheld the trial judge's denial of the defendant's motion to suppress for staleness. Id. Focusing on the characteristics of child pornography collections, the court found that the warrant application (along with testimony by the same officer during a subsequent Franks hearing) "provided considerable support for the government's position that customers of child

pornography sites do not quickly dispose of" their collection. Id. Given this support, the court found that three years was not so long a period that the information had become stale. Id.

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished). In this case, the Attorney General's Office investigated the defendant based on a tip they had received from a New Hampshire police officer. Id. at *1. Using information from online exchanges the defendant had with the officer four months prior, the AG's Office obtained a search warrant for the defendant's premises where they located the evidence at issue in this case. Id. at *1, *6. The defendant alleged that the warrant was defective because, among other reasons, "there was no temporal proximity between the events constituting probable cause and the issuance of the warrant." Id. at *5. The court rejected this argument for two reasons. First, it found that the affidavit demonstrated continuous contact between the defendant and the undercover officer for several months. Id. at *6. Even though that information was itself four months old, the court found that it gave rise to an inference that the contact had continued. Id. Second, the court focused on the special circumstance of transmitting child pornography via computer. Id. at *7. Specifically, the affidavit described how computers retain data and how collectors of child pornography tended to retain those collections for long periods. Id. The court found that these descriptions "provided the magistrate with reason to conclude that the passage of time did not constitute a disabling tardiness." Id.

(5) Timely Execution of the Warrant

Mass. Gen. Laws ch. 276, § 3A, provides that "[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event not later than seven days from the date of issuance thereof . . . ." Mass. Gen. Laws ch. 276, § 3A (2018); see also Fed. R. Crim. P. 41(e)(2)(A) (requiring return of a warrant within fourteen days in federal courts). Given the complexities inherent in searching digital devices, the requirement that warrants be executed within seven days of issue could prove burdensome when investigating computer crimes. Fortunately, Massachusetts courts have interpreted the provision liberally with regard to digital evidence, as the cases below demonstrate.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. Relying on the reasoning in Commonwealth v. Kaupp, 453 Mass. 102 (2009), the court concluded that "if police have obtained a warrant to search and seize evidence from a cell phone in their custody, they must *attempt* but need not *complete* a forensic examination of the device within seven days of the warrant's issuance," id. at 330 (emphasis added) (Commonwealth v. Kaupp is summarized below). The court provided no guidance about what exactly constituted an "attempt" to conduct a forensic examination.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it. Id. at 105–06. Though the Supreme Judicial Court invalidated the warrant on probable cause grounds, it noted that, had the warrant been valid, the fact that it took more than seven days to fully search the computer would not have required suppression. Id. at 114–15. The Court cited other jurisdictions in support of the proposition "that the police do not need to complete forensic analysis of a seized computer and other electronic data storage devices within the prescribed period for executing a search warrant." Id. at 115. The Court held that a written return listing the devices to be examined that was filed within seven days after the search warrant issued satisfied Mass. Gen. Laws ch. 276, § 3A. Id.

(6) Manner of Executing the Warrant

"Under both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, the manner in which a search is conducted must be reasonable." Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). The cases below deal with this requirement in the digital evidence context.

- Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810 (2013). This case dealt with the search of a defendant's email account after indictment, and the possibility of intercepting privileged communications. Id. at 811. The Court held that "[w]hen an indicted defendant's e-mails are the object to be searched by the Commonwealth, because there is a risk that they contain privileged communications . . . a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege." Id. The SJC distinguished McDermott in part on the ground that the warrant in that case was issued before an indictment as part of an investigation, and the Commonwealth used preset search terms during the preliminary review of the defendant's files. Id. at 831. The Court stated that it took

  > seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained.

  Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the

shooting. Id. at 751, 764–65. As part of that search, they seized computers and disks. Id. at 765. The Court upheld this seizure as reasonable because it recognized the impracticality of searching computers on-site. Id. at 776. It also analogized this seizure to that of a firearm, stating that it "must be listed in the inventory taken from the premises in the timely return of the warrant but it may be submitted for specialized examination at an off-site forensic setting for the further extraction of evidence." Id. (citation omitted). The Court stressed the need to minimize the intrusion caused by digital searches. Id. at 777. In this case, police met that burden through the procedure they employed: "A forensic duplicate was made of the . . . hard drives and storage media to preserve all original data," and investigators used a keyword search that "resulted in a cursory inspection of only approximately 750 files . . . which amounted to less than one per cent of the defendant's files." Id. The Court also suggested that "[i]n conducting the actual search . . . considerable discretion must be afforded to the executing officers regarding how best to proceed" and that "[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary." Id. at 776.

b) Exceptions to the Warrant Requirement

"Warrantless searches are per se unreasonable unless they fall within one of the few narrowly-drawn exceptions to the warrant requirement." Commonwealth v. Durham, No. 9610398, 1998 WL 34064623, at *2 (Mass. Super. Ct. Oct. 13, 1998). "When a warrantless search is conducted, the Commonwealth has the burden of showing that the search, and any resulting seizure, falls within this narrow class of permissive exceptions." Id. The sections below examine searches incident to arrest, the plain view doctrine, and exigent circumstances in the digital evidence context.

(1) Search Incident to Arrest

One of the recognized exceptions to the warrant requirement is for searches made incident to a suspect's arrest. In Massachusetts, such searches are governed not only by the Fourth Amendment and art. 14 but also by Mass. Gen. Laws ch. 276, § 1, which is generally seen as more restrictive than the Fourth Amendment. See Commonwealth v. Blevines, 438 Mass. 604, 607 (2003). This statute permits searches incident to arrest "only (1) for the purpose of seizing evidence of the crime for which the arrest has been made in order to prevent its destruction or concealment or (2) for the purpose of removing any weapon the person arrested might use to resist arrest or to escape." Id. (quoting Commonwealth v. Wilson, 389 Mass. 115, 118 (1983) (internal quotation marks omitted)).

Whether the search is permissible is based on an objective standard, so an officer's subjective intent as to the search is irrelevant as long as the search could reasonably have been expected to uncover weapons or evidence facing destruction. Id. at 608 (permitting removal of defendant's car keys from his pocket during search because an officer "discovering a hard object in [a] defendant's rear pocket, [is] justified in retrieving that object as a potential weapon"). Further, having removed an item, "police need not ignore obvious aspects of or markings on" it, id. at 609 (citing Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 770 (1989)), but "detailed scrutiny" is disallowed, id. The cases below involve digital evidence in the context of a search incident to arrest.

- Riley v. California, 134 S. Ct. 2473 (2014). In two consolidated cases, law enforcement officials inspected the contents of an arrestee's cell phone—citing the search incident to arrest (SITA) exception—and used information therefrom in aid of further investigation. Id. at 2480–82. The Supreme Court held that these searches did not fall within the SITA exception because the justifications undergirding the exception did not apply to cell phones. Id. at 2484–85. First, digital contents of a cell phone cannot pose an immediate risk of physical injury to an officer. Id. at 2485–86. Second, once the phone has been seized by law enforcement (which the Court did allow), the arrestee cannot hide or destroy any evidence thereon (at least according to the Court). Id. at 2486. Confronting the issues of automatic locking, encryption, and remote wiping, the Court expressed doubt that these issues were particularly common, drew a distinction between such actions and the arrestee-initiated destruction of evidence in a typical SITA exception case, and allowed police to employ other means of preventing such actions. Id. at 2486–88 (noting that police may power off the phone or block its network connection and hypothesizing that the police may be allowed to alter a phone's settings to prevent it from locking). Finally, the Court noted that in exceptional cases—such as an imminent threat that the phone will be remotely wiped—the exigent circumstances exception may apply on a case-by-case basis. Id. at 2487–88.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone, James provided it, and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The

image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC held that the warrantless search of the digital camera was not a valid search incident to arrest under art. 14 of the state constitution. Id. at 592–93; see also id. (declining to address the constitutionality of the search under the Fourth Amendment). The SJC applied Chimel and Riley and found the twin threats of "harm to officers and destruction of evidence" were not present with regard to the data on a digital camera. Id. at 592. The SJC reasoned that, once the camera was secured, the data on it posed no danger and the risk of destruction of evidence was mitigated (and was less of a concern with respect to digital cameras lacking network connectivity than with cell phones). Id. at 592–93.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Police apprehended the defendant after giving chase to two men. Id. at 550. Defendant claimed he was not one of the two men. Id. When asked why he was breathing heavily, he claimed to have been arguing on the phone with his girlfriend. Id. at 550–51. After he was booked, the defendant placed a phone call he claimed was to his girlfriend. Id. at 551. Police then examined his cell phone call log about five hours after the arrest, without obtaining a warrant; the log belied both of defendant's statements. Id. The booking sergeant testified that it could take several days to get a warrant, and that he was concerned that incoming calls would "push out" previous calls on the call log, which he believed permitted only a limited number of calls. Id. The SJC held that under Riley (described above), decided a year earlier, the search of the call log was not a proper search incident to arrest and was not justified by exigent circumstances. Id. at 557. The SJC found that—absent testimony suggesting the phone was password protected or that police were concerned about remote wiping—preservation of the call log could have been achieved by "turning the cell phone off, placing the cell phone in a Faraday bag, or securing the cell phone and seeking a warrant for it." Id. at 558–59.

(2) The Plain View Doctrine

Under the plain view doctrine, law enforcement may make a warrantless seizure of evidence when four conditions are met. See Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 333 (2014) (explained below). First, the officers must lawfully be in a position to view the evidence. Id. Second, they must have a lawful right of access to the object. Id. Third, they must have a reason for seizing it. Id. In cases concerning (a) items possessed illegally, the incriminating character of the object should be immediately apparent. Id. (citing Horton v. California, 496 U.S. 128, 136 (1990) (explained below)). In cases concerning (b) other types of evidence, the particular evidence must plausibly be related to criminal activity of which the police are already aware. Id. (citing Commonwealth v. Sliech-Brodeur, 457 Mass. 300, 306–307 (2010)). Fourth, art. 14 requires that police come across the object inadvertently. Id. (citing Sliech-Brodeur, 457 Mass. at 307). The following cases address the plain view doctrine in the digital evidence context.

- Commonwealth v. Tarjick, 87 Mass. App. Ct. 374 (2015). Defendant's stepdaughter disclosed he abused her and took sexually explicit photos/made recordings of her. Id. at 375. Police obtained a warrant authorizing the search of the defendant's home and the seizure of the defendant's cell phone, the family computer, and the family video camera. Id. Three memory cards that were in the camcorders or digital cameras were also seized when the warrant was executed, though they

were not included in the warrant. Id. A second warrant was obtained to search the contents of the memory cards and evidence from the cards was later used at trial. Id. at 375–76. The Appeals Court held that the seizure was within the plain view exception. Id. at 378. The cards, though not included in the original warrant, were plausibly related to the crime. Id. "The officers were . . . aware that data may be freely transferred from one device to another through memory cards, and they could reasonably have concluded that the memory cards might have contained the alleged recordings." Id. The inadvertence requirement was also satisfied because there was "no indication that the police had probable cause to believe, prior to the search, that these specific memory cards or the cameras containing them would be found." Id.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. On appeal, the court upheld this seizure under the plain view doctrine. Id. at 333. Fulfilling the first and second plain view requirements, the warrant authorizing seizure of the tank top image means the police "were lawfully situated to view and to secure the [penis] images" because police are authorized to conduct cursory inspection of computer files to determine whether they match items listed in the warrant. Id. at 333–34 (citing Commonwealth v. McDermott, 448 Mass. 750, 776–77 (2007)). Third, the images of the defendant's penis were plausibly related to criminal activity of which the police were aware. Id. at 334. The defendant's statements of intent to exchange pictures of his nude body with pictures of the minor gave police reasonable ground to believe the pictures were evidence of enticing the minor to pose in a state of nudity. Id. The same statements made it plausible that the pictures were evidence of possession of matter harmful to minors with intent to disseminate. Id. Fourth, police discovered the images inadvertently because they "lacked probable cause to believe, prior to the search, that specific items would be discovered during the search." Id. (quoting Commonwealth v. Balicki, 436 Mass. 1, 9–10 (2002)).

- United States v. Burdulis, No. 10–40003–FDS, 2011 WL 1898941 (D. Mass. May 19, 2011). Defendant in this case emailed a police officer impersonating a young boy an explicit image. Id. at *1. Police obtained a warrant to search the defendant's computer. Id. at *2. During their search of image files on the computer, police uncovered child pornography. Id. After finding the seizure of those images authorized by the initial warrant, the court held in the alternative that the plain view doctrine also authorized the use of those images in evidence. Id. at *11–12. First, the officer searching the computer was lawfully in a position to view the evidence because he was conducting a search pursuant to a warrant. Id. at *11. As he was looking for image files, he was authorized to briefly examine all images to determine if they were a match. Id. Second, by this same logic, the officer had a lawful right of access to the files. Id. at *12. Third, the prohibited nature of child pornography images would have been immediately apparent. Id. [The court did

not examine the fourth requirement—inadvertence—because it exists only under Massachusetts law. See above for more detail on inadvertence.]

(3) Exigent Circumstances

"One well-recognized exception [to the warrant requirement] applies when 'the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" Kentucky v. King, 563 U.S. 452, 460 (2011) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)). Among the exigencies that the Court has identified in the context of searching a home are "emergency aid" (entering a home to render assistance to an injured occupant), "hot pursuit" (chasing after a fleeing suspect), and the need to prevent the "imminent destruction of evidence." Id.

- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020). Police seized defendant's phone, then answered an incoming call to the phone approximately one hour and fourteen minutes after the seizure. Id. at 437–48. The Commonwealth argued that exigent circumstances justified answering the call, but it did not offer "any evidence that it was impracticable to obtain a search warrant before the call was received." Id. at 441. The court allowed defendant's motion to suppress the call and evidence derived from it, explaining that "because there [was] no evidence in the record that obtaining a warrant was impracticable here, the Commonwealth failed to meet its burden of showing exigency, and [the court was] constrained to conclude that the motion to suppress should have been allowed." Id. at 442. The court noted, however, that the burden to show that it was impracticable to obtain a search warrant in one hour and fourteen minutes was not a heavy one and could potentially have been met by an officer's testimony about the steps necessary to obtain a warrant. Id. This case indicates that courts are unlikely to treat a "one hour or two hour time frame" as *by itself* sufficient to justify a search under exigent circumstances, id. at 439, but leaves open the possibility that the same search might have been found justified had the government produced evidence showing why that short timeframe made obtaining a warrant impracticable. Id. at 442 (but see Alvarez, 480 Mass. 1017 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer and absent any argument by the defendant that "observation of the outside of the… phone constituted a search")).

- Commonwealth v. Cruzado, 480 Mass. 275 (Aug. 10, 2018). Police found a cell phone lying near the defendant in a stairwell. Id. at 282. Having probable cause, the police seized the cell phone. Id. The Supreme Judicial Court held that "exigent circumstances supported the warrantless seizure: the risk of someone taking or tampering with the cell phone. Left unattended, especially in an area to which many people had access, the cell phone would have been at the risk of theft or vandalism." Id. at 283.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Possible degradation of a call log on a cell phone was deemed not an exigent circumstance because such degradation could be prevented in a number of different ways, such as by turning off the phone. Id. at 558–59.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's (a teacher) computers in a school classroom. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized both computers and subsequently obtained a search warrant. Id. at 105. The Court upheld the seizure of defendant's computer as appropriate because of exigent circumstances. Id. at 105–06. Specifically, the Court noted that "impoundment of an object pending the issuance of a search warrant violates the Fourth Amendment . . . only if it is unreasonable," which "turns on the facts of each case, requiring courts to 'balanc[e] the need to search or seize against the invasion that the search or seizure entails.'" Id. at 106 (quoting Commonwealth v. Catanzaro, 441 Mass. 46, 55–56 (2004)). The Court held that "[g]iven the ease with which computer files may be accessed and deleted, and the disruption that would have been created by posting an officer in the defendant's office and preventing students from entering pending the issuance of a search warrant . . . the seizure was reasonable." Id. In a footnote, the Court noted that while exigent circumstances justified the seizure, they would not have justified the subsequent search had it been warrantless because "[t]he exigency necessitating [the computer's] seizure dissipated once the computer had been secured." Id. n.7.

(4) Emergency Aid Exception

The emergency aid exception to the warrant and probable cause requirements originated in the context of searching a home, "permit[ting] the police to enter a home without a warrant when they have an objectively reasonable basis to believe that there may be someone inside who is injured or in imminent danger of physical harm." Commonwealth v. Peters, 453 Mass. 818, 819 (2009). The exception has since been extended to "uphold warrantless searches of places other than homes, in order to find and assist a victim of serious physical harm or to prevent such harm from occurring," and most recently to searches of the digital information. Commonwealth v. Raspberry, 93 Mass. App. Ct. 633, 639-40 (2018).

- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018). Police officers listening to a wiretap had "grave concerns about the defendant imminently causing serious bodily harm" to another with a firearm. Id. at 635 (internal quotation marks omitted). To locate the defendant and prevent the harm, police "asked AT&T to perform 'emergency pings' and give the police real-time CSLI about the approximate location of the defendant's cell phone." Id. The Commonwealth did not contest that a Fourth Amendment "search" took place, instead arguing that the "search" was "reasonable" under the emergency aid doctrine. See id. at 638, 640. The Massachusetts Appeals Court agreed. See id. at 641 ("We have no difficulty concluding that these standards were met here . . . What police did not know here, at the time of the call, was the whereabouts of the defendant. In the circumstances, it was objectively reasonable for the police to request real-time CSLI, in order to determine the defendant's current location and the direction in which she was moving, and thus to find and intercept her before she could shoot Dorsey.").

The emergency aid exception differs from the exigent circumstances exception: the former requires no probable cause to conduct a search, whereas the latter permits a warrantless search where probable cause exists but the circumstances make obtaining a warrant impracticable. Raspberry, 93 Mass. App. Ct. at 638, n. 8.

(5) Inventory Exception

Seizures of items on an arrestee's person may also be permissible, subject to police inventory policies. "[B]efore a person is placed in a cell, the police, without a warrant, but pursuant to standard written procedures, may inventory and retain in custody all items on the person . . . ." Commonwealth v. Seng, 436 Mass. 537, 550 (2002). For such seizure to be lawful, police must follow the rules of a written inventory policy that is "explicit enough to guard against the possibility that police officers would exercise discretion with respect to whether to open closed [containers] as part of their inventory search." Commonwealth v. Rostad, 410 Mass. 618, 622 (1991). "Inventory searches are intended to be noninvestigatory and are for the purpose of safeguarding the defendant's property, protecting the police against later claims of theft or lost property, and keeping weapons and contraband from the prison population." Barillas, 484 Mass. at 256. As such, "[i]n making an inventory — taking from the person, noting what is received, and placing it in safekeeping — the police are to act more or less mechanically, according to a set routine, for to allow then a range of discretion in going about a warrantless search would be to invite conduct which by design or otherwise would subvert constitutional requirements." Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 772 (1989) (cited in Barillas, 484 Mass. at 259).

Investigatory use of items seized under the inventory exception is impermissible unless the police have a search warrant or "obtain consent from the appropriate person (as determined by the inventory policy)." Barillas, 484 Mass. at 257. Any evidence resulting from investigatory use of inventory items without consent or a warrant is subject to suppression. Id.

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC rejected the argument that the search of the camera was a valid inventory search, holding that it was instead investigatory in nature because the camera was suspected stolen and the search was meant to identify the owner. Id. at 595–96.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found the defendant hiding in his home, conducted a pat frisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to

unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

(6) Consent

Warrantless searches are permissible with appropriate advance consent.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure was lawful under the search incident to arrest exception. Id. at 255.However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable

expectation of privacy in his movements. Id. at 77. The Court further held that the consent search of the defendant's residence was tainted by the illegal CSLI search. Id. at 71. Believing that the defendant and a second individual were transporting narcotics from Florida to Massachusetts, police obtained a court order pursuant to 18 U.S.C. § 2703 (2006) requiring the second individual's cellular service provider to "ping" the location of his cell phone. Id. at 73-74. After the two returned to Massachusetts, police knocked on the defendant's door and told him they knew he had just "purchased a large amount of narcotics" in Florida and was possibly storing it at his apartment. Id. at 74. The defendant then consented to a search, and police discovered a large amount of cash and two bricks of cocaine in his residence. Id. at 75. The SJC considered three factors in determining whether the defendant's consent was attenuated from the tainted CSLI data: "(1) the amount of time that elapsed between the defendant being confronted with the illegally obtained CSLI evidence and his grant of consent; (2) the presence of any intervening circumstances during that time period; and (3) the purpose and flagrancy of the official misconduct." Id. at 81-82 (internal quotes omitted). As to factors (1) and (2), the Court held that the lack of time and intervening events between the acquisition of the CSLI data and the police officer's confrontation with the defendant claiming that he had just returned from Florida with drugs weighed heavily against attenuation. Id. at 82-83. As to factor (3), while the Court "recognize[d] that the illegal police misconduct here was neither purposeful nor flagrant," it was still not dispositive in attenuating defendant's consent from the tainted CSLI data. Id. at 84. In her dissent, Justice Cypher explained that she would not reach the conclusion of the majority that a passenger in a tracked car has standing to challenge a CSLI search. Id. at 86 n.1 (Cypher, J., concurring in part and dissenting in part). In addition, she encouraged the SJC to adopt the good faith exception to the exclusionary rule in cases where the police acted under a "reasonable good faith belief that their conduct was lawful at the time." Id. at 92. While Justice Lowy agreed that Massachusetts should adopt a good faith exception, he did not believe the issue was properly raised by the Commonwealth in this case. Id. at 85-86 (Lowy, J., concurring).

3. The Exclusionary Rule

Generally, the exclusionary rule prohibits the introduction of evidence obtained as a result of a violations of the Fourth, Fifth and Sixth Amendments to the U.S. Constitution, and their counterparts under the Massachusetts Declaration of Rights. See Commonwealth v. Lora, 451 Mass. 425, 439 & n.26 (2008).

a) Good Faith / Substantial and Prejudicial

The Supreme Court has limited the application of the exclusionary rule in federal cases where officers acted in good faith, but Massachusetts does not recognize the good faith exception under art. 14. See Commonwealth v. Porter P., 456 Mass. 254, 273 (2010). Instead, it looks to "the foundational purpose of the rule—to deter unlawful police conduct . . . as a guiding principle" to determine whether evidence should be excluded. Commonwealth v. Maingrette, 86 Mass. App. Ct. 691, 697 (2014) (citing Commonwealth v. Wilkerson, 436 Mass. 137, 142 (2002)). Where:

> an arrest is wrongly made on the basis of mistaken information chargeable solely to the police, the burden is on the government to show . . . that the [government's] mistake was reasonable in the circumstances, and that the violation was minor or insubstantial and nonprejudicial and that exclusion of the evidence would not be likely to deter future police misconduct.

Id. (citations omitted).

b) Inevitable Discovery

> "Under the inevitable discovery doctrine, if the Commonwealth can demonstrate by a preponderance standard that discovery of the evidence by lawful means was certain as a practical matter, the evidence may be admissible as long as the officers did not act in bad faith to accelerate the discovery of evidence, and the particular constitutional violation is not so severe as to require suppression."

Commonwealth v. Fontaine, 84 Mass. App. Ct. 699, 709 (2014) (citation omitted). Though there are no Massachusetts cases applying this doctrine to a computer search, the First Circuit case below applying a slightly different federal test is instructive:

- United States v. Crespo-Rios, 645 F.3d 37 (1st Cir. 2011). In this case, the FBI searched the defendant's computer and external hard drive for evidence of chats between both him and an undercover agent and him and minors. Id. at 40–41. The search for these chats was conducted pursuant to a warrant that also listed, among other things, child pornography as something being sought. Id. at 40. During this search, agents found child pornography. Id. Following his indictment, the defendant moved to suppress the evidence, arguing that there was insufficient probable cause to support the overly-broad search warrant. Id. at 41. The First Circuit overturned the lower court by applying the inevitable discovery doctrine. Id. at 42-44. In searching the computer and hard drive for the chat evidence—for which there was undoubtedly probable cause—the court found that government agents would inevitably have discovered the child pornography because searching for computer files allows brief scanning of all possibly relevant files on the computer. Id. [This analysis is quite similar to that of the plain view doctrine, discussed elsewhere in this guide.]

B. Search of Electronic Service Providers

1. General Overview of Stored Communications Act

In 1986, Congress enacted the Stored Communications Act (SCA). See Pub. L. 99-508, 100 Stat. 1848, Title II. It provides limited privacy protections to the customers of "electronic communication service[s]" (ECS) and "remote computing services" (RCS). Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 383 (2014). ECS providers are email services like Gmail or Yahoo! along with certain elements of social media platforms, like a user's Facebook "wall." See generally Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 8–11 (2013).

RCS providers are harder to define and include any company that provides "computer storage or processing services by means of" the Internet to the public. Pub. L. 99-508, 100 Stat. 1848, § 2710. Cloud storage providers like Dropbox clearly fit this definition. Jeffrey Paul DeSousa, Self-Storage Units and Cloud Computing, 102 Geo. L.J. 247, 250 n.19 (2013). Courts have also found that YouTube belongs in this category. Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 11 (2013).

For a discussion of the argument that text messaging services are "remote computing services" under 18 U.S.C. § 2703(b) see Commonwealth v. Fulgiam, 477 Mass. 20, 31–33 (2017). The SJC held that the Commonwealth may not obtain the content of text messages without a warrant because text messaging is an "electronic communication service" subject to the requirements of § 2703(a). Id. at 32–33. The SJC also decided that a warrant supported by probable cause was also required for the content of text messages under art. 14. Id. at 33–34.

2. Search warrants served on out-of-state Internet service providers

Out-of-state corporations providing ECS or RCS to Massachusetts residents are subject to the jurisdiction of Massachusetts courts and must comply with search warrants issued by them. See Mass. Gen. Laws ch. 276, § 1B (2018); see also 18 U.S.C. § 2703 (2018) (outlining process by which state courts exercise jurisdiction over ECS and RCS providers).

C. Encryption and Self Incrimination

1. The Foregone Conclusion Doctrine

The Fifth Amendment to the United States Constitution states, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." This does not mean that a defendant cannot be compelled to produce some types of incriminating evidence, however, because only compelled *testimonial* communication that incriminates is barred. See Commonwealth v. Gelfgatt, 468 Mass. 512, 519 (2014) (citing Fisher v. United States, 425 U.S. 391, 408 (1976)). Written or oral communication created in response to government demand is plainly testimonial. See id. at 520. Compelled action that communicates something can also be testimonial in nature. Id.

"Whether an act of production is testimonial depends on whether the government compels the individual to disclose 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Gelfgatt, 468 Mass. at 520 (quoting United States v. Hubbell, 530 U.S. 27, 43 (2000)). For example, giving blood, producing a voice exemplar, or standing in a lineup are all nontestimonial because the suspect in question "is not required to disclose any knowledge he might have, or to speak his guilt." Id. at 521 (citations omitted). By contrast, complying with the government's demand could be testimonial "where [the act of production] is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence." Id. (citing Hubbell, 530 U.S. at 36 & n.19).

Even in cases where the act of producing evidence that the government seeks to compel is testimonial, however, that production loses its testimonial character if the information that would be

disclosed by the production is a "foregone conclusion." Id. at 522. The forgone conclusion exception obtains "where the facts conveyed already are known to the government, such that the individual 'adds little or nothing to the sum total of the Government's information.'" Id. (quoting Fisher, 425 U.S. at 411). In other words, "the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production." Commonwealth v. Jones, 481 Mass. 540, 547 (2019).

Several State and Federal courts have "applied the foregone conclusion exception in the context of compelled decryption," but neither the United States Supreme Court nor the Circuit Courts of Appeal have ruled on the government's burden of proof that applies to the "foregone conclusion" exception under the Fifth Amendment. Jones, 481 Mass. at 550. One federal district court "concluded that the appropriate standard of proof under the Fifth Amendment is clear and convincing evidence. Id. (citing United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018).

- In re a Grand Jury Investigation, 92 Mass. App. Ct. 531 (2017). During a grand jury investigation, a judge ordered petitioner to enter his personal identifying number (PIN) access code into his iPhone smartphone. Id. at 532. A warrant had previously issued for a search of the phone. Id. The Appeals Court held that production of the PIN was within the foregone conclusion exception to the Fifth Amendment. Id. at 534. To meet its burden under the doctrine, the prosecution had to demonstrate knowledge of the ownership and control of the cell phone and its contents, as well as "knowledge of the fact of [PIN code protection], and knowledge of the [existence of the PIN code]." Id. (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 524 (2014)). The prosecution was not required to show that it knew the specific content of the cell phone, but it did need to demonstrate knowledge of the existence and the location of the content. Id.

Article Twelve (art. 12) of the Massachusetts Declaration of Rights—analogous to the Fifth Amendment—provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself." Article Twelve provides greater protection than the Fifth Amendment in some contexts, but this broader protection "does not change the classification of evidence to which the privilege applies," so only "testimonial or communicative" evidence is protected from compelled disclosure. Commonwealth v. Gelfgatt, 468 Mass. 512, 525 (2014) (citations omitted). Massachusetts also recognizes the "foregone conclusion" exception to art. 12. Id. at 526.

For the exception to apply in the context of an order compelling decryption of an electronic device, Article Twelve requires that "the Commonwealth . . . prove beyond a reasonable doubt that the defendant knows the password." Commonwealth v. Jones, 481 Mass. 540, 552. But the Commonwealth does not need to "prove any facts with respect to the contents" of the device to be decrypted. In addition, "the entry of the password alone does not convey the fact of 'ownership' of the device or its contents." Id. at 547 n.8.

2. Encryption

In an affidavit the Commonwealth submitted in Gelfgatt, the director of the Massachusetts Attorney General's computer forensics laboratory explained that "encryption" is:

> the process by which 'readable' digital media, that is, digital media or data that can be viewed and accessed, is scrambled in such a way as to render that digital media or data 'unreadable' without decryption. Encryption can be performed both by hardware and by means of software tools.

Commonwealth v. Gelfgatt, 468 Mass. 512, 516 n.9 (2014). The director described "decryption" as:

> the process by which encrypted, scrambled data is rendered 'readable' again. In order to decrypt data, the person seeking decryption performs some action such as the entering of a password, scanning of a fingerprint or [insertion of] a USB Thumb drive with a pass code key on it. The encryption software then translates this action into a 'key,' essentially a string of numbers or characters. The encryption software then applies this key to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again.

Id. In Gelfgatt, the Commonwealth represented that the defendant's encryption software was virtually impossible to decrypt. Id. at 516–17. The Commonwealth represented that files thus encrypted could only be viewed if an authorized user entered a password. Id. at 517. But compelling the user to enter or disclose their password presents a possible violation of the Fifth Amendment and art. 12. The Gelfgatt court examined the interplay of these issues in Massachusetts:

- Commonwealth v. Gelfgatt, 468 Mass. 512 (2014). Defendant in this case was allegedly involved in a mortgage fraud scheme. Id. at 513. Law enforcement believed proof of that scheme would be found on the defendant's computers, and they obtained a search warrant, but encryption on the computers foiled their search. Id. at 516–17. When interviewed by police, the defendant admitted to owning multiple computers, stated that the police would be unable to access them because they were encrypted, and stated that he was able to decrypt the computers but refused to do so. Id. at 517. The lower court found that compelling him to do so would violate his Fifth Amendment and art. 12 rights against self-incrimination. Id. at 518–19. The SJC reversed and held that he could be compelled to enter his password in the circumstances presented by this case. Id. at 519–26.

  > First, the Court stated that compelling a defendant to enter a decryption password, in the abstract, implicated the Fifth Amendment because the defendant would be implicitly "acknowledging that he has ownership and control of the computers and their contents," which could itself be relevant to the Commonwealth's case against him. Id. at 522. Next, the Court considered the "foregone conclusion" exception (explained above) and held that it applied because the defendant had already admitted to owning multiple computers, that their contents were encrypted, and that he was capable of decrypting them. Id. at 523-24. As a result, the facts that would have been communicated by compelling him to decrypt the computers were already known to the government,

making them a foregone conclusion. Id. Finally, the Court examined the issue under art. 12 but held that the same analysis applied. Id. at 524–26. [Note: Crucially, the Commonwealth proposed a protocol for decrypting the files that limited the scope of what was communicated through the compelled decryption. That protocol is outlined above.]

- Commonwealth v. Jones, 481 Mass. 540 (2019). Defendant was charged with trafficking a person for sexual servitude, Mass Gen. Laws ch. 265, § 50(a) (2018); id. at 541, and deriving support from the earnings of a prostitute, Mass. Gen. Laws ch. 272, § 7 (2018); id. at 541. The Commonwealth seized an LG cell phone from the defendant at his arrest and later obtained a warrant to search the phone. Id. at 541, 544. The LG phone had to be decrypted with the entry of a password before the search could be executed. Id. at 541. The Commonwealth moved for a Gelfgatt order, compelling the defendant to decrypt the LG phone under the "forgone conclusion" exception to the privilege against self-incrimination under the Fifth Amendment to the U.S. Constitution and Article 12 of the Massachusetts Declaration of Rights. Id. at 541–42. The SJC found that in order to obtain a Gelfgatt order compelling a defendant to decrypt an electronic device, the Commonwealth must "prove that the defendant knows the password beyond a reasonable doubt for the foregone conclusion exception to apply." Id. at 542–43. The Court also concluded that the Commonwealth met its burden in this case. Id. at 543. Finally, the SJC concluded that judges can consider new information in deciding renewed Gelfgatt motions, "without first finding that [the new information] was not reasonably available to the Commonwealth at the time the earlier Gelfgatt motion was filed." Id.

  To meet its burden of proving beyond a reasonable doubt that the defendant's knowledge of the password was a "foregone conclusion," the Commonwealth offered the following evidence: a witness testified to the defendant's regular use of the LG phone to answer calls and communicate through text messages (the record revealed several communications between the witness's phone and the LG phone related to prostitution); the defendant's phone number was listed with his name in the witness's contacts; the LG phone was in the defendant's possession at the time of arrest; the defendant had characterized the telephone number of the LG phone as his number to police when he was being booked following an arrest in an unrelated matter; police records showed that a backup number listed for the LG phone was registered to a person with the same name, social security number, and date of birth as the defendant; CSLI records revealed that the LG phone was in the same location at the same time as another phone that was found to be the defendant's phone. Id. at 556–57. All of this evidence, "taken together with the reasonable inferences drawn therefrom, prove[d] beyond a reasonable doubt that the defendant [knew] the password to the LG phone." Id. at 557 (noting that "it is hard to imagine more conclusive evidence" showing that the defendant knows the LG phone's password). The SJC also noted that even if the LG phone was used by more than one person, proof of ownership or exclusive control was not required. Id. at 547 n.8.

3. Sample Decryption Protocol

In Commonwealth v. Gelfgatt, the Commonwealth employed the following protocol to limit the amount of information that would be communicated by the compelled decryption:

> 1. The defendant, in the presence of his counsel, shall appear at the [Digital Evidence Laboratory] of Massachusetts Attorney General [Maura Healey] within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
>
> 2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
>
> 3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
>
> 4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
>
> 5. The defendant is expressly ordered not to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program;
>
> 6. The Commonwealth shall not view or record the password or key in any way; [and]
>
> 7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter.

Id. at 517 n.10.

D. Searches Implicating Attorney-Client Privilege

Searches that may intercept privileged communications between a suspect and his lawyer should be handled with special care. See generally Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 811 (2013). This problem is especially acute when a search is executed after a suspect has already been indicted and retained counsel. See, e.g., id. Even when a post-indictment search targets a different crime than the one for which the defendant was indicted, such a search runs a risk of encountering

privileged communications. Id. at 817–18. The section below detail how such a search should proceed in Massachusetts.

1. Post-Indictment Email and File Searches

The Commonwealth may seize emails of a defendant under indictment by means of an ex parte search warrant. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 821–22 (2013). Because of the sensitive nature of such a seizure, however, "only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment." Id. at 822. The affidavit supporting the warrant application must inform the judge at the outset that the subject of the email search is under indictment and must explain the connection, if any, between the indictment and the search warrant being sought. Id. Finally, the affidavit must explain why a search warrant rather than a rule 17(a)(2) summons is necessary to obtain the emails. Id. One possible explanation the SJC has suggested is cases where the Stored Communications Act requires a warrant, which it does for emails not yet opened that are 180 or less days old. See id. at 819 n.17 (citing 18 U.S.C. § 2703(a)), 822.

Once seized, emails possibly containing privileged material may be searched only after the Commonwealth receives a Superior Court judge's approval of a search protocol including specific procedures to protect against searches of privileged communications between a defendant and his attorneys. Id. at 823. One such procedure that the Court has approved is laid out below in the "Taint Team" section.

2. Taint Teams

A "taint team" is a group of attorneys or agents employed by a government office who have not at any time been involved in the investigation and/or prosecution of the defendants and who will not be assigned to any such investigation or prosecution in the future who sort the defendant's communications into privileged and unprivileged so that the latter group may be investigated by the government without eroding a defendant's attorney-client privilege. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 824–25 (2013).

There is "widespread skepticism" about the ability of government agents to properly review privileged communications without affecting that privilege, id. at 825, but the SJC has concluded that taint teams can "offer adequate protection to the Commonwealth's citizens," id. at 827. To that end, the SJC has put in place a two-tiered set of requirements surrounding the use of taint teams.

First, before a judge may authorize a team that will use members of a prosecutor's office as its members, "the Commonwealth must establish the necessity of doing so" because "use of an independent special master offers a far greater appearance of impartiality and protection against unwarranted disclosure and use of an indicted defendant's privileged communications." Id. at 829. In ruling on the prosecution's request to use a taint team, "the judge may consider factors such as the number of documents to be searched, the relative cost of a special magistrate, and the Commonwealth's unique ability to perform such a search due to specialized computer forensic examiners in its employ." Id. Further, the judge will consider "the Commonwealth's ability to erect an impenetrable wall between members of the taint team and members of the prosecution team." Id. at 829–30. In making this

determination, the judge will consider "the size of the particular prosecutor's office," and the Court expressed "less confidence that a small District Attorney's office can screen off members of the taint team as effectively as the Attorney General's office may be able to do." Id. at 830.

> Second, to pass constitutional muster, the taint team must comply with each of four requirements:
>
> (1) the members of the taint team must not have been and may not be involved in any way in the investigation or prosecution of the defendants subject to indictment—presently or in the future; (2) the taint team members are prohibited from (a) disclosing at any time to the investigation or prosecution team the search terms submitted by the defendants, and (b) disclosing to the investigation or prosecution team any e-mails or the information contained in any e-mails, subject to review until the taint team process is complete and in compliance with its terms; (3) the defendants must have an opportunity to review the results of the taint team's work and to contest any privilege determinations made by the taint team before a Superior Court judge, if necessary, prior to any e-mails being disclosed to the investigation or prosecution team; and (4) the members of the taint team must agree to the terms of the order in writing.

Id. at 828.

3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails)

"'Generally, disclosing attorney-client communications to a third party undermines the privilege.'" Dahl v. Bain Capital Partners, LLC, 714 F. Supp. 2d 225, 227 (D. Mass. 2010) (quoting Cavallaro v. United States, 284 F.3d 236, 246–47 (1st Cir. 2002)).

"'An exception to this general rule exists for third parties employed to assist a lawyer in rendering legal advice,'" including CC'ed emails. Id. at 227 (quoting Cavallaro, 284 F.3d at 247). In order for the exception to obtain, three criteria must apply: (1) the communication must be "necessary, or at least highly useful" for effective consultation between client and lawyer; (2) the exception only applies if the third party is playing an interpretive role between the lawyer and client (e.g., an accountant if he is helping the lawyer understand complex financial information); and (3) the communication must be made for the purpose of rendering legal advice, and not business advice or otherwise. Id. at 227–28.

II. Evidentiary Matters

A. Judicial Discretion

1. Trial Judge's Discretion

"A judge has broad discretion in the admission" of "demonstrative aids, including digital photographs and computer-generated images." Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing Commonwealth v. Noxon, 319 Mass. 495, 536 (1946)).

For an example of related flawed evidentiary practice, see Commonwealth v. Mienkowski, 91 Mass. App. Ct. 668 (2017). At a trial for aggravated rape of a child, posing a child in a state of nudity, and of dissemination of matter harmful to minors, the defendant's cell phone was admitted into evidence. Id. at 669. After some initial ambiguity about how the jury could examine the phone during deliberation, the judge adopted the Commonwealth's position and instructed the jury to limit their examination to the evidence already admitted (screenshots of relevant text messages). Id. at 675–77. On appeal, the defendant argued that the judge's initial admission of the cell phone without limitation and statements he made at the charge conference led defense counsel to rely in her closing on the jury's ability to examine the cell phone unconstrained and then "cut the legs out from under" her argument. Id. at 677–78. The SJC found it was possible that "neither the litigants nor the judge fully had considered the plethora of difficult issues that may be raised when a cell phone containing troves of unidentified electronic data is delivered into a jury's hands." Id. at 678. Though it held that it would have been preferable to resolve the ambiguity earlier, the SJC found no reversible error in the judge's handling of the issue. Id. at 678–69.

2. Demonstrative Photographs

"When, as here, the demonstrative photograph is generated as a digital image or video image, the judge must determine whether the image fairly and accurately presents what it purports to be, whether it is relevant, and whether its probative value outweighs any prejudice to the other party." Renzi v. Paredes, 452 Mass. 38, 52 (2008) (citing Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006)). "Concerns regarding the completeness or production of the image go to its weight and not its admissibility." Id. (citing Leneski, 66 Mass. App. Ct. at 295–96).

B. Discovery

1. Pornographic Images in Child Pornography Cases

"That forensic examination of the computer data by an expert retained by the defense is an essential component of effective assistance of counsel" in a child pornography case "is self-evident." Commonwealth. v. Ruddock, No. 08–1439, 2009 WL 3400927, at *3 (Mass. Super. Ct. Oct. 16, 2009). If an expert's access to evidence for purposes of examination is limited to the Commonwealth's facilities in order to prevent dissemination of such materials, the defendant's right to effective assistance of counsel will be unduly burdened. Id. A copy of the mirror image of a seized drive, including pornographic

images, must be given to the defendant's counsel of record and expert forensic examiner under a protective order limiting access to defense counsel and the expert. Id. (citing Mass. R. Crim. P. 14(a)(6)).

2. Wiretap transcripts

- Commonwealth v. Tavares, 482 Mass. 694 (2019). The defendant was convicted of murder in the first degree. During the investigation, police had recorded conversations between the defendant and a confidential informant using a wiretap. Id at 698. Prior to trial, the defendant moved successfully to suppress the recordings because "the investigation was not in connection in with organized crime" and thus violated G. L. c. 272, § 99. Id. at 714. After he was convicted, the defendant filed a motion for a new trial, arguing that his counsel was ineffective for failing to seek suppression of evidence derived from the recordings, as well as a "motion for postconviction discovery to obtain copies or transcripts of the wiretap recordings." Id at 714. The trial court denied both motions. Id. "Under the Massachusetts wiretap statute, a criminal defendant 'may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom' if the interception was made in violation of the statute." Id at 715 (quoting G. L. c. 272, § 99). On appeal, the SJC affirmed denial of the ineffectiveness motion, ruling that the defendant "failed to identify any specific evidence admitted at trial that was derived from the unlawful recordings." Id. But the Court reversed the denial of the motion for post-conviction discovery, concluding that the defendant is entitled to a copy of the wiretap transcript prior to any retrial. Id. at 715-716. The SJC found that the transcript would enable defense counsel to examine whether there is any improper reliance on the suppressed recordings at any future trial. Id.

3. Cell phone data

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.). The defendant, indicted on one count of rape, filed a Mass. R. Crim. P. 17(a)(2) motion to obtain information from the victim-witness's cell phone relating to her electronic communications and use of social media over a twelve-day period beginning with the day of the incident. Id. at *2–3. The motion judge ordered the victim-witness to produce her cell phone and/or any "backups" for forensic examination to recover the sought-after information. Id. at *3. The judge also ordered that the victim-witness provide the names and login information for third-party service providers that possessed the information, and directed Facebook to provide Facebook and Instagram data associated with the victim-witness's accounts, including photographs and the contents of messages. Id. The victim-witness, joined by the Commonwealth, petitioned a single justice of the Supreme Judicial Court for relief from the order under G.L. c. 211, § 3, asking that (1) the twelve-day period for which cell phone data was sought be more narrowly tailored to the time of the incident, and (2) the order be vacated insofar as it required the victim-witness to provide the names and login information for third-party service providers. Id. The single justice granted the requested relief. First, the justice summarized the Lampron requirements for a successful Rule 17 motion: relevance, admissibility, necessity, and specificity. Id. at *4. The justice then noted that Massachusetts case law had yet to address the use of Mass. R. Crim. P. 17 to obtain a victim-witness's cell phone communications or third-party service providers. Id. Observing that "individuals have significant privacy interests at stake in their cell phones," the justice concluded

that, "when ruling on a request under Rule 17 for a victim-witness's cell phone or cell phone records, the judge must include a consideration of these inherent privacy concerns." Id. The justice also examined decisions in which other state and federal courts had confronted similar issues, including a Minnesota Supreme Court decision holding that the fact that a "cell phone could contain exculpatory information was insufficient to order its production for examination." Id. at *5 (citing In re B.H., 946 N.W.2d 860, 870-71 (Minn. 2020)). Finally, the justice noted that Rule 17 "is a rule of production, not a rule of discovery." Id. After taking the above factors into account, and in light of the fact that the defendant could only speculate that relevant evidence might be obtained from the broad sweep of sought-after information, the justice granted the victim-witness's requested relief.

C. Authentication

1. Generally

To find that evidence is authentic, a judge must determine whether, by a preponderance of the evidence, there is sufficient evidence, including "confirming circumstances," to permit a "reasonable jury to conclude that this evidence is what the proponent claims it to be." Commonwealth v. Purdy, 459 Mass. 442, 449 (2011). Confirming circumstances are other facts that imply that evidence is what the proponent represents it to be. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011).

2. Photographs and Digital Images, Videos, and CDs

Authentication of photographs and videos is "typically… done through one of two means—having an eyewitness testify that the [photo or] video is a fair and accurate representation of what he saw on the day in question, or having someone testify about the [recording] procedures and the methods used to store and reproduce the [photo or] video material." Commonwealth v. Connolly, 91 Mass. App. Ct. 580, 586 (2017) (citing Commonwealth v. Pytou Heang, 458 Mass. 837, 855 (2011); Commonwealth v. Rogers, 459 Mass. 249, 267 (2011)). Digital photographs and videos are treated as equivalent to their analog counterparts. See Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294–95 (2006).

These are not the only possible ways to authenticate photo and video evidence, however. Commonwealth v. Davis, 97 Mass. App. Ct. 633, 635–36 (2020). More generally, admissibility may be established by any "evidence sufficient to support a finding that the matter in question is what its proponent claims." Mass G. Evid. § 901(a). For example, a witness may authenticate a digital photograph or video by testimony about the process used to create it and "showing that it produces an accurate result." Mass. G. Evid. § 901(b)(9).

- Commonwealth v. Davis, 97 Mass. App. Ct. 633 (2020): An officer at the scene of a crime saw a surveillance camera mounted on the outside of a nearby building, aimed at the street intersection where the crime had occurred. Id. at 635. He spoke with a resident of the building, viewed a video recording taken by the surveillance camera, and learned that the camera had been pointed at the intersection at the time of the crime. Id. Neither the resident nor the officer knew how to transfer the surveillance video recording to another medium, so Carty used his cellphone to record a video of the surveillance video recording; this cellphone video was played to the jury. Id. The following

was held sufficient to authenticate the cellphone video: the officer testified (1) that he had seen the scene that appeared in the video ("a car, with its driver's side door open, that had crashed into a pole at the intersection of Quincy Street and Baker Avenue"); (2) that the surveillance camera was aimed at the intersection in question, and (3) that still photographs also in evidence were fair and accurate representations of the scene of the shooting, where the still photographs depicted multiple vehicles and a sign that also appeared the video. Id. at 636.

- Commonwealth v. Leneski, 66 Mass. App. Ct. 291 (2006): A witness sufficiently authenticated a CD containing digital images created by a digital camera system at a convenience store where that witness testified he had "viewed the images on the computer and 'burned' the CD copy; [and] testified as to the procedure he used in the surveillance process, the copying process, and to the contents of the CD." Id. at 295.

Testimony about a photo or video that is not introduced in court, but instead is described to the jury by a witness, is subject to the admissibility conditions as the original photo or video: that is, the testimony is admissible upon establishing that the photo or video the witness saw was a fair and accurate representation of the events in question. Commonwealth v. Connolly, 91 Mass. App. Ct. at 586–87.

3. Digitally Enhanced Images and Video

The SJC has indicated that even digital photographs that have been enhanced have some use as a demonstrative aid, so long as they accurately illustrate what a witness testifies about. See Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing 2 McCormick, Evidence § 214 (6th ed. 2006)).

When offering digitally enhanced photographs or videos, the type of media and the manner of enhancement will be relevant. See Iacobucci v. Boulter, 193 F.3d 14, 20 (1st Cir. 1999). Objections to evidence on the grounds that it lacks a proper foundation are allowed at the discretion of the judge. Id. In Iacobucci, where the audio portion of a video was enhanced with a high quality play-back system to increase the volume, the trial judge decided that this did not destroy the video's integrity and the video was properly authenticated. Id. Several witnesses positively identified the defendants' voices on the recording, and the jury had the opportunity to evaluate the identification on their own. Id. at 20–21.

Alternatively, "[f]or digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007). In such a case, there will need to be proof that the digital enhancement process produces reliable and accurate results. Id.

4. Transcripts of Recordings

A written transcript of a recorded conversation taken from an electronic transmitting device can be authenticated where a witness testifies that the transcript is a fair and accurate representation of the recording. See United States v. Anderson, 452 F.3d 66, 76–77 (1st Cir. 2006) (citing United States v. Ademaj, 170 F.3d 58, 65 (1st Cir. 1999)). That witness does not have to be the person who transcribed the recording. Id. at 77.

5. Email

"While e-mails and other forms of electronic communication present their own opportunities for false claims of authorship, the basic principles of authentication are the same." Commonwealth v. Purdy, 459 Mass. 442, 450 (2011) (citing United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006)). Email authentication does not require expert testimony or evidence of exclusive access or password protection, although they are relevant to the jury's assessment of the weight of the evidence. See id. at 451. Where the relevance or admissibility of emails depends on whether the defendant authored the emails, the judge must "determine whether the evidence [is] sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the e-mails." Id. at 447 (citing Commonwealth v. Leonard, 428 Mass. 782, 785–86 (1999); Mass. G. Evid. § 104(b)(1)).

However, where the contents of an email do not sufficiently authenticate it, it may be properly authenticated through confirming circumstances. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011). Confirming circumstances imply that evidence is what the proponent represents it to be. Id. at 674. For example, the following confirming circumstances were sufficient to link a defendant to emails: (1) an email revealed that the sender would meet the email recipient at a certain place and time, and the defendant then appeared in that place at the time specified; (2) the sender of that email included his telephone number and a photograph of himself. Id. at 674–75. The defendant answered a call to that number, and emailed photograph depicted the defendant. Id.

Other confirming circumstances include: (1) emails originate from an account that bears the defendant's name and that the defendant admits having used; (2) emails are found on a computer hard drive that the defendant admits owning; (3) the defendant supplies all necessary passwords to access files on the computer; (4) emails contain an attached photograph of the defendant and/or describe the unusual circumstances or traits attributable to the defendant. Purdy, 459 Mass. 442, 450–51 (2011).

"Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking website such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant. There must be some confirming circumstances sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the emails." Id. at 450 (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)); see also Griffin v. State, 419 Md. 343, 357–58 (2011) (holding that authentication of a page printed from a social networking site requires more than a showing that a picture, birth date, and location of the alleged creator exist on the profile from which the page was retrieved).

Embedded e-mails will not be excluded because of the mere possibility that they can be altered without any specific evidence showing alteration. In Safavian, when "the trustworthiness of the emails particularly those . . . . emails that are included in a chain-either as ones that have been forwarded or to which another has replied" were challenged, the district court held that the "*possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course any more than it can be the rationale for excluding paper documents (and copies of those documents)."

435 F. Supp. 2d at 41 (emphasis in original). The court added that the defendant would be entitled, however, to raise any issue of alteration with the jury. Id.

6. Chatrooms

Similar to the method of authentication by confirming circumstances allowed in the Commonwealth, "[c]ourts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. For example, in [the Pennsylvania case] In re F.P., the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert . . . . The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 556 (D. Md. 2007) (citing In re F.P., 878 A.2d 91, 93–94 (Pa. Super. Ct. 2005)).

7. Text Messages

- Commonwealth v. Alden, 93 Mass. App. Ct. 438 (2018). The victim received threatening text messages from a "telephone number [she] had used to communicate with the defendant . . . every few days for over one year." Id. at 439. The trial court held that "the Commonwealth had established by a preponderance of the evidence that the text messages were authentic" - i.e., that the messages came from the defendant. Id. at 440. The Massachusetts Appeals Court affirmed because "for over one year, [the victim] had contacted the defendant multiple times each week using the telephone number from which the threatening messages originated. When she called that number, the defendant answered. When she sent a text message to that number to arrange a meeting with the defendant, he appeared." Id. at 440–41. Moreover:

> [t]he content of the text messages reinforced their link to the defendant. It is undisputed that at the time she received the text messages, [the victim] was a witness in a pending case against the defendant. In this context, where there was evidence that the text messages directed her to "keep her [explicative] mouth shut" and "leave their personal stuff out of the courtroom" or "people [would] come after [her] if [she] went to court," it was reasonable to infer that the defendant was responsible for sending the messages.

  Id. at 441.

8. Information Available on Websites and Social Networks

Evidence available on websites presents its own problems. "Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007). "The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting." Id. (citing United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000)). In doing so, federal courts require the proponent of such evidence to show what was actually on the website, to show that the

exhibit or testimony accurately reflects that content, and to show that the content can be attributed to the owner of the site. Id. (citations omitted).

In the courts of the Commonwealth, "[e]vidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant." Commonwealth v. Purdy, 459 Mass 442, 450 (2011) (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)).

Circumstantial evidence can authenticate a social network page:

- Commonwealth v. Meola, 95 Mass. App. Ct. 303, No. 18-P-83, 2019 WL 2202909 (Mass. App. Ct. May 22, 2019). The Appeals Court affirmed the Superior Court's holding that sufficient evidence in the form of "confirming circumstances" established that the defendant attached an obscene video to a communication he sent to an underage victim. Following a jury waived trial, a Superior Court judge found the defendant guilty of disseminating obscene material to a minor in violation of G.L. c. 272, § 28. Id. at *1. The Appeals Court looked to the principles established by the SJC in Commonwealth v. Purdy, 459 Mass 442 (2011) regarding authenticating digital evidence (that is not self-authenticating). First, Purdy establishes that direct evidence is not necessary to determine that a defendant sent a digital communication. Rather, a judge "may consider circumstantial evidence and look to 'confirming circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored" the electronic communication. Meola, 2019 WL 2202909 at *5 (quoting Purdy, 459 Mass. at 450). Second, under Purdy, the "mere possibility that a digital communication was fraudulently sent by someone other than the person associated with a particular social media...account from which the communication originated is not a bar to its authentication." Meola, 2019 WL 2202909 at *5. Third, common-law principles concerning authenticity are applicable to digital communications. Id. In this matter, the trial judge's decision to exclude records proffered by the prosecutor, describing user information related to the Facebook account and the sender of the video, required the Commonwealth to rely on indirect evidence to authenticate the materials. Id. at *2. The Appeals Court concluded that the following facts offered sufficient indirect evidence of authenticity: the defendant's prior association with the victim (defendant had previously lived with her and her mother); the defendant's biological relation to the victim's half-sister; and the friend request the user of the account sent to the victim. Moreover, the Court determined that the trial judge did not err in finding the communications authentic because there was no evidence to suggest that the Facebook profile photo or the self-authored obscene video were publicly available. Id. at *6. Based on these facts, the Court affirmed the trial judge's determination that the defendant "purposefully disseminated matter harmful to a minor to the victim" with full knowledge that she was a minor. Id. at *7.

- Other jurisdictions have taken a similar approach. For example, in the Texas case Tienda v. State, MySpace webpages were admissible because there was sufficient evidence on them indicating that they "were what they purported to be." 358 S.W.3d 633, 646 (Tex. Crim. App. 2012). The court stated that, "as with the authentication of any kind of proffered evidence, the

best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case." Id. at 639. The court held that there was "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the Myspace pages belonged to the appellant and that he created and maintained them." Id. at 645; see also Parker v. State, 85 A.3d 682 (Del. 2014) (holding that social media post was sufficiently authenticated by circumstantial evidence and by testimony explaining how the post was obtained); Simmons v. Commonwealth, No. 2012–SC–000064–MR, 2013 WL 674721 (Ky. Feb. 21, 2013) (holding that the print-outs of the defendant's Facebook messages were admissible because the messages were what they purported to be and the role of the judge, as a gatekeeper, was only to determine if an offering party has produced enough evidence for a reasonable jury to find authenticity).

9. Software Programs Used in Investigation

When a witness uses software to create information relevant to an investigation, that witness should testify in detail as to the nature of the tool, how the witness used it, and how it was created and maintained in order to authenticate the records. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 327 (2009) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)). In Whitlock, a police officer used a software program called ArcView, which is a computerized map that depicted the location and ownership of property within the city of Springfield. Id. at 325–26. The information provided by this software was used to show that the defendant was distributing a controlled substance within a school zone. Id. Where software provides information to a witness, for example software that measures and provides distances between real-world objects, it does not make a "statement," and therefore is not subject to the hearsay rule. Id. at 326–27.

10. GPS and Probation

The SJC has held GPS technology to be "widely used and acknowledged as a reliable relator of time and location data" under the Daubert-Lanigan standard for admission of scientific testimony. Commonwealth v. Thissell, 457 Mass. 191, 198 (2010); see also Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592-3 (1993); Commonwealth v. Lanigan, 419 Mass. 15, 26 (1994). Judges may at their discretion admit testimony that "GPS data placed the defendant in particular locations at particular times" based on data from any GPS device whose positioning method has been demonstrated to be "no more than the application of existing and scientifically-accepted GPS monitoring technology -- a technology that has been accepted as reliable." Davis, 97 Mass. App. Ct. at 640. The fact, acknowledged by an appellate court, that GPS information is "subject to variations in accuracy depending upon atmospheric conditions, intervening obstacles, or reflection of the satellite signals from buildings, windows, or cars, [goes] to the weight of the evidence, not to the fundamental reliability of the GPS technology." Id. (citing Sacco v. Roupenian, 409 Mass. 25, 30 (1980); Rothkopf v. Williams, 55 Mass. App. Ct. 294, 299 (2002)). An appellate court has distinguished and left unresolved the issue of whether GPS records are also reliable indicators of speed (as opposed to location). Id. at 641.

Probationers' GPS records have been used as evidence of a defendant's location at particular times; evidence that can be relied on to show that the defendant violated conditions of probation or was at

the scene of a crime. Thissell, 457 Mass. at 198–99; Davis, 97 Mass. App. Ct. at 639–40. Official GPS records maintained by the Commonwealth and certified by an officer having legal custody of the record may minimize concerns about authenticity, Thissell, 457 Mass. at 199 ("recommend[ing] strongly that copies of GPS records offered in future revocation proceedings be properly attested and certified by an appropriate custodial officer"), but GPS-based information may also be authenticated on other ways. Davis, 97 Mass. App. Ct. at 637 (authenticating GPS data by the testimony of a GPS device manufacturer's manager of product development).

D. Technological evidence as the basis of criminal conviction

Evidence used as the basis of a conviction must be sufficient, viewed in the light most favorable to the government, for a rational trier of fact to find the essential elements of the crime beyond a reasonable doubt. Commonwealth v. Ayala, 481 Mass. 46, 51 (2018) (citing Commonwealth v. Latimore, 378 Mass. 671, 677-78 (1979). Thus, even evidence that meets the preponderance standard required to authenticate a piece of evidence, see § II.C, supra, may not be sufficient to support a conviction. The government bears the burden of explicit proof even for facts about technology that may be well known to the trier of fact, e.g., that a password is generally required to log in to and send messages from an Instagram account. Commonwealth v. McMann, 97 Mass. App. Ct. 558, 561 (2020). Such facts are not appropriate subjects of judicial notice. Id. at 561 n.4.

- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020). Defendant was convicted of violating an abuse prevention order that prohibited him from contacting his ex-girlfriend. Id. While the order was in effect, the ex-girlfriend received an Instagram message from user "bigm617" that said "Yoooo." Id. at 559. She testified that she knew that "bigm617" was the defendant's account "because the associated account displayed pictures of the defendant, including one of him with the victim, and the victim and the defendant had previously 'liked' and commented on each other's Instagram posts." Id. The victim showed this Instagram message to a police officer, who met with the defendant later that day. Id. The defendant denied sending any message to the victim, 'wanted to show [the officer] that he never did[,]' and entered a passcode to unlock his cell phone. He then opened the Instagram application on his cell phone, and the 'Yoooo' message to the victim appeared on the screen. The officer observed that the defendant looked '[s]urprised.' Id. The appeals court held that "even assuming without deciding that the Instagram message was properly authenticated, the Commonwealth failed to… prov[e] beyond a reasonable doubt that the defendant was the person who wrote or sent the message to the victim. Although the evidence was sufficient to show that the Instagram account was the defendant's and that he could access it, there was no circumstantial evidence establishing authorship." Id. at 560. The court suggested the burden could have been met by "evidence that the message itself contained characteristics showing that the defendant wrote it, or through evidence establishing how secure Instagram accounts are and how the Instagram cell phone application works." Id. at 562.

E. Best Evidence Rule

1. Best Evidence Rule - Generally

"The best evidence rule provides that, where the contents of a document are to be proved, the party must either produce the original or show a sufficient excuse for its nonproduction." Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001); see also Mass. G. Evid. § 1002. However, what constitutes a "document" has been narrowly construed such that "[t]he best evidence rule is applicable only to those situations where the contents of a *writing* are sought to be proved." Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970) (emphasis added). Most photographs and videos depict objects rather than writings. Consequently, the best evidence rule does not typically apply, *inter alia*, to photographs or videotapes. See also Commonwealth v. Weichell, 390 Mass. 62, 77 (1983) (holding that the "enlarged photograph was a fair and accurate representation of the defendant at the time of his arrest"); Commonwealth v Leneski, 66 Mass. App. Ct. 291, 294 (2006) ("Videotapes, like photographs, are not subject to the best evidence rule."). Additionally, "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes." Leneski, 66 Mass. App. Ct. at 294.

2. Digital Images

Digital image evidence is not subject to the best evidence rule in Massachusetts because these images are not writings. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006) (citing Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970)). The Leneski court held that digital images from a computer copied to a compact disk ("CD") would be considered as originals. Id. Testimony about authenticity, including how the disc was generated, the procedure used in the surveillance process, the copying process, and the contents of the CD, was deemed sufficient. Id. The Court noted that there was opportunity for cross-examination that went to the weight of the evidence on the subject of surveillance procedure and the method of storing and reproducing the data. Id.

This exception to the best evidence rule extends to images that have been transferred from a hard drive to other media such as CDs and DVDs. See id. at 294 (holding that "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes").

3. Admission of Duplicate Evidence

> [W]here the original [of a document] has been lost, destroyed, or otherwise made unavailable, its production may be excused and other evidence of its contents will be admissible, provided that certain findings are made.
>
> As a threshold matter, the proponent must offer evidence sufficient to warrant a finding that the original once existed. . . . If the evidence warrants such a finding, the judge must assume its existence, and then determine if the original had become unavailable, otherwise than through the serious fault of the proponent . . . and that reasonable search

> had been made for it. . . . If the judge makes these findings in favor of the proponent, the judge must allow secondary evidence to establish the contents of the lost writing.

Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001) (quoting Fauci v. Mulready, 337 Mass. 532, 540–43 (1958) (internal citations and quotation marks omitted)).

4. Videos

The best evidence rule does not apply to digital videos. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006). "Our courts have held that videos are 'on balance, a reliable evidentiary resource . . . .'" Id. (quoting Commonwealth v. Harvey, 397 Mass. 351, 359 (1986)). "[Videos] 'should be admissible as evidence if they are relevant, they provide a fair representation of that which they purport to depict, and they are not otherwise barred by an exclusionary rule.'" Id. (quoting Commonwealth v. Mahoney, 400 Mass. 524, 527 (1987)).

5. Email

It is unlikely that printed email communications are subject to the best evidence rule so long as their authenticity can be proven through circumstantial evidence. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 675–76 (2011). In Amaral, the court reasoned that the email server, or the computer itself, is not better evidence than directly printed emails, and that "[t]he significance of the best evidence rule has declined appreciably in recent decades." Id. at 675 (internal quotation marks omitted).

6. Summaries

Large volumes of digital evidence may be summarized and shown to a jury without running afoul of the best evidence rule.

In the Commonwealth, voluminous evidence that would be difficult for a jury to understand due to volume or complexity may be presented in the form of a written or testimonial summary or a chart, shown by testimony to accurately reflect the contents of the underlying documents, so long as the proponent does not unfairly emphasize portions of the summarized evidence. See Mass. G. Evid. § 1006; Commonwealth v. Mimless, 53 Mass. App. Ct. 534, 538 (2002) (quoting Welch v. Keene Corp. 31 Mass. App. Ct. 157, 165–66 (1991)) ("[C]are must be taken to insure that summaries accurately reflect the contents of the underlying documents and do not function as pedagogical devices that unfairly emphasize part of the proponent's proof.") (internal quotation marks omitted); Commonwealth v. Greenberg, 339 Mass. 557, 582 (1959) ("The witness was not allowed to state deductions and inferences of his own but could state only the results of his computations from the admitted evidence."). The summarized evidence should be made available to other parties in advance of trial, and the court may order that the originals be produced in court. See Mass. Guide to Evid. § 1006.

- Commonwealth v. Suarez, 95 Mass. App. Ct. 562 (2019). The defendant, who was convicted of assault with intent to rape and other charges, challenged on appeal the introduction at trial of a six-minute compilation of video surveillance footage from before, during and after the attack, and a timeline describing parts of the videos. Id. at 566-67, 570. Since the defendant did not object at

trial, the Appeals Court "examine[d] whether any abuse of discretion in admitting the exhibits created a substantial risk of a miscarriage of justice." Id. at 570-71. The Court found the individual underlying videos could not 'be conveniently examined in court.'" Id. at 571 (quoting Mass. G. Evid. § 1006). Though the Commonwealth played portions of the videos in the courtroom, "a deliberating jury would have found it difficult to master the technology necessary to find and view the relevant parts of the videos in the jury room." Id. at 571-72. Furthermore, the Court rejected the defendant's claim that the compilation was unfairly edited. Id. at 572. However, the Court did find certain improprieties in the compilation and timeline. In particular, it ruled that still photos, taken from a 7-Eleven store four hours after the attack, should not have been included in the compilation because the photos taken hours after the assault were not relevant to the crime itself. Id. The Court also ruled that the timeline describing the digital compilation "could and should have used a neutral heading" for a set of video clips. Id. at 574. The Court criticized the Commonwealth's use of the term "suspect" in the timeline to refer both to a person the defendant admitted was him, in certain video clips, and to the attacker, in other video clips, since use of that term suggested that they were the same person. Id at 573. The Court ruled, however, that these "limited errors in the compilation and the timeline" did not create a substantial risk of a miscarriage of justice because they had little, if any, impact on the case. Id. at 574.

F. Hearsay

When software merely provides information to a witness, the software does not make a "statement," and therefore is not subject to the hearsay rule. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326–27 (2009) (holding that information provided by measuring software that indicated to the witness the distance between real-world objects were not statements subject to the hearsay rule) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)); see also Thissell, 457 Mass. at 197 n.13 (discussing the difference between computer-generated and computer-stored records in the context of the rule against hearsay); Commonwealth v. Royal, 89 Mass. App. Ct. 168, 171–72 (2016) (treating "computer-stored" records as hearsay, but treating "computer-generated" records as not hearsay); Commonwealth v. Woollam, 478 Mass. 493, 498 (2017) (holding that call logs are computer-generated records that do not raise hearsay concerns; admissibility thus only depends on authentication); Davis, 97 Mass. App. Ct. at 641–43 (holding that GPS logs and maps of the defendant probationer's location over time, which were created by a mapping company that added dots and the defendant's name to maps based on GPS location data, were not hearsay).

G. Business Records Exception

1. Email

A document from an email service provider that indicates that a specific login name is connected to a defendant's email address is admissible as a business record as long as it is supported by an affidavit from the service provider's custodian of records. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 673–74 (2011).

2. Computer Records

"[C]omputer records . . . are admissible under the business records exception to the hearsay rule, [Mass. Gen. Laws ch.] 233, § 78, if they were (1) made in good faith; (2) made in the regular course of business; (3) made before the action began; and (4) [it was] the regular course of business to make the record at or about the time of the transaction or occurrences recorded." McLaughlin v. CGU Ins. Co., 445 Mass. 815, 819 (2006) (quoting Beal Bank, SSB v. Eurich, 444 Mass. 813, 815 (2005) (internal quotation marks omitted)).

A lack of personal knowledge on behalf of the affiant, the maker, or custodian of records goes to the weight and not the admissibility of the business records. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674 (2011) ("[T]he personal knowledge of the entrant or maker affects only the weight of the record, not its admissibility.") (quoting and citing Note to Mass. Guide to Evid. § 803); see also McLaughlin, 445 Mass. at 819 (2006) ("[P]ersonal knowledge of the entrant or maker of a record is a matter affecting the weight rather than the admissibility of the record.").

A print-out of an electronic document is admissible as a business record as long as it is supported by an affidavit from the provider's custodian of record establishing that the requirements of the business records exception are met. Amaral, 78 Mass. App. Ct. at 673–74 n.4; McLaughlin, 445 Mass. at 8199 ("The affidavits plainly establish that the records satisfy these foundational requirements.").

H. Confrontation Clause

1. Software-generated information

"The confrontation clause bars the admission of testimonial out-of-court statements by a declarant who does not appear at trial unless the declarant is unavailable to testify and the defendant had an earlier opportunity to cross-examine him." Commonwealth v. Wilson, 94 Mass. App. Ct. 416, 417 n.1 (2018), (quoting Commonwealth v. Simon, 456 Mass. 280, 296 (2010).

When introducing software-generated information that is not hearsay as evidence, see § II.E, supra, the Confrontation Clause is not implicated. See Commonwealth v. Hurley, 455 Mass. 53, 65 n. 12 (2009) ("admission of a testimonial statement without an adequate prior opportunity to cross-examine the declarant… violates the confrontation clause only if the statement is hearsay…") (citing Crawford v. Washington, 541 U.S. 36, 59-60 & n. 9 (2004).

It is unclear whether the introduction of software-generated information that *is* hearsay (if that is possible at all) would implicate the Confrontation Clause. An appellate court has considered the question in dicta, and suggested that (1) software-generated information may not come from a "declarant" within the meaning of the Confrontation Clause at all, but (2) if a company involved in producing the information were treated as a declarant, then the requirements of the Confrontation Clause could be satisfied by having a representative of the company as a witness. Davis, 97 Mass. App. Ct. at 644.

2. Secondary Examiners

The Sixth Amendment's bar on the testimonial statements of a witness who does not appear at trial applies to forensic examiners because their explanation of the process and results of specific forensic examinations are testimonial statements. See United States v. Soto, 720 F.3d 51, 58–60 (1st Cir. 2013) (summarizing relevant Supreme Court cases).

A "surrogate" witness who is familiar with a lab's practices, but who has formed no independent opinion of the results is insufficient to satisfy the Sixth Amendment. Id. at 58 (citing Bullcoming v. New Mexico, 564 U.S. 647, 662–63 (2011)).

However, "[t]he government may ask an agent to replicate a forensic examination if the agent who did the initial examination is unable to testify at trial, so long as the [testifying] agent . . . conducts an independent examination and testifies [as] to his own results." Id. at 59; see, e.g., Commonwealth v. Chappell, 473 Mass. 191, 199–200 (2015) (substitute DNA expert testimony allowed because, as the second reader, she independently read all the raw data and the reports produced by the original analyst, made interpretations, and ensured that there was agreement between her findings and those the analyst, and therefore testified to her opinions or conclusions concerning the DNA).

- Commonwealth v. Seino, 479 Mass. 463 (2018). Defendant was convicted of first-degree murder. Id. at 464. On appeal, he asserted several confrontation claims. Id. at 466, 469–72. First, the defendant argued that it was improper for a doctor who did not perform the autopsy to refer during his trial testimony to statements in the autopsy report and death certificate, neither of which the testifying doctor authored. Id. at 466. The SJC held that it was appropriate for the testifying doctor to offer his opinion on the cause of death based on the case file and his own examination, but agreed with the defendant that the doctor should not have testified about statements in the autopsy report and death certificate. Id. at 466–67. The SJC found that the error was harmless beyond a reasonable doubt, however, because the improper testimony was cumulative, did not incriminate the defendant, and "did not contribute to the guilty verdicts." Id. at 467–68. Second, the defendant argued that his confrontation right was violated when two experts, as part of their trial testimony, used charts showing DNA testing data obtained by other analysts (who did not testify). Id. at 469–70. The SJC held that the data should not have been shown to the jury. Id. at 470. The Court also concluded, however, that there was no substantial likelihood of a miscarriage of justice "because the charts did not taint the analysts' independent opinions, which . . . were properly admitted." Id. at 471. [Note: The Court applied a miscarriage of justice standard because the defendant did not preserve an objection to the charts at trial. Id. at 470.] The SJC noted that the charts "merely displayed genetic locations, not any information regarding a match or the statistical probability thereof." Id. at 471. Third, the defendant argued that it was reversible error for an analyst to testify that the defendant's DNA profile matched a DNA profile developed by a different analyst from the victim's jeans. Id. The SJC rejected this claim, finding that the defendant had had the opportunity at trial to cross-examine the analyst who developed the defendant's DNA profile, the supervisor of the laboratory that developed the DNA profile from the jeans, and the analyst who compared the two profiles. Id. at 471–72.

- Commonwealth v. Scesny, 472 Mass. 185 (2015). An autopsy report and photographs from the victim's autopsy were introduced in evidence and a substitute medical examiner testified regarding findings in the report. Id. at 196–97. The SJC held the autopsy report was "'inadmissible hearsay whose admission violate[s] the defendant's right of confrontation under the Sixth Amendment to the United States Constitution,'" id. at 197 (quoting Commonwealth v. Emeny, 463 Mass. 138, 145 (2012)), and that a substitute medical examiner cannot testify about the facts and findings of the report on direct examination. Id. The autopsy photographs were properly admitted through a State police trooper who attended the autopsy. Id. at 198 n.25.

- Commonwealth v. Jones, 472 Mass. 707 (2015). At defendant's trial for rape, a chemist at the State police crime laboratory, who was not present during the "rape kit" examination and had no apparent connection to the hospital at which the swabs were taken, was allowed to testify on direct examination to her "understanding" of how the swabs had been collected. Id. at 711–12. The SJC held that allowing an expert witness who had not been present during the examination and had no apparent connection to the hospital where the examination occurred, to testify on direct examination to her "understanding" of how the swabs had been collected violated the defendant's confrontation right. Id. at 708. The SJC found that the "surrogate" expert's statements were testimonial for two main reasons: (a) in labeling the various swabs and completing the "rape kit" inventory list, the initial examiner made factual statements concerning how the swabs were collected, and (b) the purpose of a "rape kit" is to gather forensic evidence for use in a criminal prosecution,. Id. at 714. These statements would therefore only be admissible if they complied with the test established by Commonwealth v. Greineder, 464 Mass. 580, 593 (2013). Id. at 715. The Jones Court summarized the holding of Greineder as follows: "'[e]xpert opinion testimony, even if based on facts and data not in evidence, does not violate the right of confrontation, provided that the facts and data 'are independently admissible and are a permissible basis for an expert to consider in formulating an opinion,' and that two further conditions are met. First, the expert must 'not present on direct examination the specific information on which he or she relied'; second, the expert witness must have the capacity to 'be meaningfully cross-examined about the reliability of the underlying data.'" Id. at 713 (quoting Greineder, 464 Mass. 580) (other citations omitted). The statements in Jones did not meet either of these requirements in Greinder: (1) the underlying hearsay facts of how the swabs were collected came in on direct examination and (2) the expert could not meaningfully be cross-examined about the reliability of the representations of the "rape kit" examiner concerning the origins of the swabs and lacked the capacity to address chain of custody and evidence-handling protocols relevant to the process by which the swabs were collected. Id. at 715–16. The testimony thus failed to comply with Greineder and was therefore inadmissible. Id. at 715.

III. Cybercrimes

A. Possession of Child Pornography

1. Multiple Convictions Require Multiple "Caches"

In prosecuting possession of child pornography, each "cache" of pornography counts as one unit of prosecution. See Commonwealth v. Rollins, 470 Mass. 66, 73–75. That is, "a defendant's possession of a single cache of one hundred offending photographs in the same place at the same time gives rise to a single unit of prosecution pursuant to [Mass. Gen. Laws ch. 272,] § 29C" rather than one-hundred separate charges and convictions. Id. at 74. To support multiple prosecutions for possession of child pornography in compliance with the Double Jeopardy Clause, that possession must be "'sufficiently differentiated by time, location, or intended purpose.'" Id. at 73 (quoting Commonwealth v. Rabb, 431 Mass. 123, 130 (2000) (with internal quotation marks omitted)).

- Commonwealth v. Wassilie, 482 Mass. 562 (2019). The defendant, who was convicted on 15 separate indictments relating to secretly videotaping nude or partially nude adults and children, appealed, arguing that the judge erred in ruling that the proper units of prosecution were the individual victims rather than the individual episodes of surveillance. Id. at 563. The defendant concealed his cell phone in a unisex, one room bathroom without stalls at an angle that gave a clear view of the toilet. Id. at 563-564. He recorded two videos on the same day, and these videos captured "genitalia of children and adults, male and female"—a total of seventeen adults and five juveniles. Id. On appeal, the Court cited precedent that, for the purpose of determining whether particular conduct constitutes a single offense or multiple offenses, there are two categories of statutes. Id. at 567. "One category is focused upon the prevention of violence or physical injury to others." Id. In this category, a single incident can give rise to multiple indictments, based on the number of victims. Id. The other category is directed at "punishing the defendant for conduct offensive to society." Id. For this second category, separate indictments for separate victims are not appropriate. Id. at 568. Some crimes, like the one at issue here, do not fit neatly into either category. Id. The defendant argued that the statute reflects an intent to punish the physical act of recording, but the Court read the statute as punishing criminal acts that invade an individual's privacy. Id. The Court also rejected the defendant's reasoning on the grounds that his statutory interpretation would produce the "absurd result" of allowing people who take illicit photos of multiple people to be tried as if they had one victim. Id. at 571. Based on this statutory analysis, the Court upheld the lower court's decision to use a per victim unit of prosecution. Id. at 578.

2. Brief Possession is Sufficient

Brief possession of offending images is sufficient to sustain a violation of Mass. Gen. Laws ch. 272, § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 329–30 (2011). Evidence of prolonged or continued control is not needed. Id. (citing Commonwealth v. Harvard, 365 Mass. 452, 458 (1969)). In Hall, although the defendant's cell phone no longer contained child pornography and though there was no confirmation that the defendant had viewed the pictures sent to him by the victim, the defendant was

found guilty of possession of child pornography because the fact that he had enticed and encouraged the victim combined with the fact that he received the images allowed a jury to find that he had possessed them. Id. at 327–29.

3. Receipt by Cell Phone is Sufficient

Confirmation that defendant's cell phone received picture messages from the victim, where the defendant enticed the victim to take and send the picture messages, is sufficient to show control and possession of such photos in violation of Mass. Gen. Laws ch. 272 § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 327–29 (2011).

4. Malware and Computer Viruses Defense

The First Circuit notes that "we must be cognizant of 'the prevalence and sophistication of some computer viruses and hackers that can prey upon innocent computer users' by placing child pornography on their machines, but 'the specter of spam, viruses, and hackers must not prevent the conviction of the truly guilty.'" United States v. Rogers, 714 F.3d 82, 87 (1st Cir. 2013) (quoting United States v. Pruitt, 638 F.3d 763, 766–67 (11th Cir. 2011)). In Rogers, the possibility that the child pornography found on the defendant's computer was a result of malware was ruled out by forensic analysis (where an analyst installed the same malware on another computer and no child pornography was found) and corroborating evidence (child pornography found on another computer, browsing history matching an interest in child pornography, and evidence that some of the pornography had been deleted by the defendant). Id.

5. Probable cause / Staleness in Child Pornography Cases

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that the probable cause in the affidavit in support of the warrant to search his home was stale. Id. In Guastucci, police were investigating the upload of a single image of child pornography from the defendant's home to Skype seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time, the Court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the Court separately identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant

affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]", an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

B. Statutory Terms of Mass Gen. Laws ch. 272

1. "Dissemination"

"The definition of 'disseminate' includes 'publish, produce, print, manufacture, distribute, . . . exhibit or display.' The statutory emphasis is on the content of the material and the intent of the person disseminating such material; the draftsmen were not so much concerned with the manner in which the image was distributed, exhibited, or displayed. The statutes criminalize such dissemination whether accomplished by way of hand, mail, facsimile, or through the use of e-mail. The judiciary ought, absent constitutional inhibitions, give effect to the purpose of the law gleaned from the Legislature's choice of language." Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *2 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 31 (internal citation marks omitted)).

"Possession" is not an element of the crime of "dissemination." Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *4 (Sep. 22, 2016) (unpublished). To "disseminate" is defined as 'to import, publish, produce, print, manufacture, distribute, sell, lease, exhibit or display." Id. at *5 (quoting Mass. Gen. Laws ch. 272, § 31). In Moore, the appeals court held that "[t]o infer a requirement of possession would be to add a requirement not expressed by the Legislature." Id. The term "dissemination" also connotes some form of distributive act beyond showing something to another. Id. Consider Commonwealth v. McDonagh, 480 Mass. 131 (2018), where the defendant showed nude pictures on his computer to his minor son. The Commonwealth charged the defendant with various offenses, including dissemination of obscene matter (in violation of Mass. Gen. Laws ch. 272, § 29). Id. at 132. On appeal, the Commonwealth conceded that the evidence was insufficient to prove "dissemination." Id. at 144–45.

2. Computer "Depictions"

"The Legislature was unconcerned with how the photographically created image is stored or communicated." Commonwealth v. Hall, 80 Mass. App. Ct. 317, 326 (2011). "[T]he Legislature's creation of a separate and distinct category for 'depiction by computer' manifests an intent to give special treatment to the unique issues presented by computers, including the fact that stored data, although intangible in their unprocessed form, are readily transferrable to a graphic image." Id. at 327 (quoting Mass. Gen. Laws ch. 272, § 29C).

"Depiction by computer," as that phrase is used in § 29C, includes an unopened file on a hard drive—not only a file that is reduced to a hard copy, or one that is disseminated. Commonwealth v. Hinds, 437 Mass. 54, 63–64 (2002).

3. Child Enticement

"[I]n order to constitute enticement of a victim, the defendant need not physically meet the victim at the same place to which he entices the victim to go" given modern and electronic digital technology. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 323 (2011). In Hall, the Appeals Court noted that the defendant's enticement of the victim via cell phone text messages to go to a private place and take naked photographs to send to him can qualify as enticement. Id. However, given the potentially duplicative offense of posing a child in a state of nudity, the court held that the defendant must lure the child to a place of his/her choosing, not the victim's choosing. Id at 324–25. As this element was missing in Hall, the defendant's enticement charge was set aside. Id. at 325.

4. "Visual Material"

"The Legislature's objective of including a broad range of 'visual material' in its proscription is further demonstrated by Section 31's second sentence which provides: '[u]ndeveloped photographs, pictures . . . and similar visual representations or reproductions may be visual materials notwithstanding that processing, development or similar acts may be required to make the contents thereof apparent.' Thus, in determining whether an image is a 'visual material' within Mass. Gen. Laws ch. 272, the manner of its dissemination is insignificant. Whether further acts are required to make the image apparent to the naked eye, by, for example, keying a computer board, does not render the image any less a 'visual material.'" Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *3 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 29C).

5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31

The SJC examined the definition of "nudity" under §31 in Commonwealth v. Provost, 418 Mass. 416 (1994). In this case, the defendant took photographs of children in the pool and boys in the locker room. Id. at 417–18. One child struck different poses and his partially covered scrotal area was visible in two photographs. Several others showed the child displaying his bare buttocks ("mooning" the defendant). Id. at 418. The SJC provided the following analysis of the statutory meaning of "nudity": "The defendant claims that his activities do not fall within the ambit of § 29A(a). He first contends that the photographs do not depict a minor in a state of nudity within the meaning of, which defines 'nudity' as: 'uncovered or less than opaquely covered human genitals, pubic areas, . . . or the covered male genitals in a discernibly turgid state.' Although [the child] had his underwear on, in two of the photographs portions of his pubic and genital area are clearly visible. The statute does not require that the areas be completely uncovered. It is enough that a portion of the genital area is visible." Id. at 418 (quoting Mass. Gen. Laws ch. 272, § 31).

6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A

A "performance" under Mass. Gen. Laws ch. 272, § 29A "does not expressly or implicitly require the physical presence of 'one or more persons.' In view of the advances in technology, a violation of the statute may occur without the defendant's physical presence." Commonwealth. v. Bundy, 465 Mass. 538, 545 (2013) (finding the statutory definition of performance satisfied by victim masturbating facing a

camera attached to a device that, through an Internet connection, resulted in the image being broadcast to the defendant for him to view).

A "performance" occurs "before one or more persons" even when the only audience member is the person who enticed or encouraged the performance because to hold otherwise would circumvent the plain meaning of "one." Id. at 544.

7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A

Mass. Gen. Laws ch. 272, § 29A(b), provides in relevant part: "Whoever . . . hires, coerces, solicits or entices, employs, procures, uses, causes, encourages, or knowingly permits such child to participate or engage in any act that depicts, describes, or represents sexual conduct for the purpose of representation or reproduction in any visual material, or to engage in any live performance involving sexual conduct, shall be punished . . . ." (quoted in Com. v. Bundy, 465 Mass. 538, 539 n.2 (2013)). In Bundy, the jury was instructed as follows on a charge under this statute:

> [I]n proving [the element of live performance], the Commonwealth must establish beyond a reasonable doubt that it was [the defendant's] specific intent to solicit, entice, cause, or encourage [the victim] to engage in a live performance involving sexual conduct. In determining whether the defendant possessed such a specific intent, [the jury] may consider all facts and circumstances, including the defendant's acts and statements. The statute also permits the Commonwealth to establish alternatively that the defendant knowingly permitted [the victim] to engage in a live performance involving sexual conduct.

Id. at 542.

The meaning of "knowingly permit" was at issue in Commonwealth. v. Provost, 418 Mass 416 (1994). The defendant in Provost asserted that "the depiction of [a victim's] pubic area was unintentional and that, since [the victim] voluntarily struck the various poses without instruction, [defendant] did not 'knowingly permit' him to pose in a state of nudity." Id. at 419. The court rejected this argument and held that:

> The photographs themselves suggest that the defendant knowingly permitted [the victim] to pose with a portion of his pubic region and genitals exposed. He took a series of well-focused photographs at various points in the process of [the victim's] dressing. [The victim's] genital area is prominent in many of the photographs. The defendant admitted that he sometimes took photographs of nude boys for sexual gratification. There was sufficient evidence, therefore, for the judge to conclude that the defendant knowingly permitted [the victim] to pose in a state of nudity. Furthermore, the fact that the defendant continued to take the photographs as [the victim] struck different poses certainly supports the inference that he "encouraged" [the victim] to pose in a state of nudity.

Id. at 419.

8. Lewdness

In Commonwealth v. Rex, 469 Mass. 36 (2014), during a standard cell inspection prisoner Rex was found in possession of seven photographs of naked children. Id. at 37. The photos were from National Geographic, a sociology textbook, and a naturist catalogue. Id. The Court held that the indictment for possession of child pornography was properly dismissed because the children depicted were not in unnatural poses and their genitals were not the focus of the photo. Id. at 47. Thus the photos did not depict lewdness—just nakedness. Id. at 47–48. "It is well settled that nudity alone is not enough to render a photograph lewd." Id. at 44 (quotation omitted).

C. Special Conditions of Probation

Special conditions of probation can be unconstitutionally vague — facially or as applied — if they do not give fair notice to a defendant of the scope of prohibited activity. Commonwealth v. Ruiz, 453 Mass. 474, 479 (2009). A defendant "cannot be found in violation of probationary conditions that might have been intended or would have made sense, only of those that are unambiguous and of which he has notice," Commonwealth v. King, 96 Mass. App. Ct. 703, 710(2019) (citing Commonwealth v. Lally, 55 Mass. App. Ct. 601, 603 (2002)), and "ambiguities in probation conditions are construed in favor of the defendant." Lally, 55 Mass. App. Ct. at 603 (citing Commonwealth v. Power, 420 Mass. 410, 421 (1995)).

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography." Id., at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. The court found this sufficed to put the defendant on fair notice that possession of "explicit stories describing the rapes of young children" would violate his probation. Id. at 786-87. However, the court found that a reasonable person would not consider photographs of adults in their underwear or with their hands covering their genitals to be pornographic. Id. Therefore, they were not "so inarguably pornographic as to put the defendant on fair notice that he was violating probation by possessing them," where the photographs "depicted no sexual activity or nudity, and it [was] unclear whether the intent behind them was to arouse sexual excitement." Id. at 786.

  Commonwealth v. King, 96 Mass. App. Ct. 703 (2019). Defendant, who had pled guilty to possession of child pornography, was subject to special probation conditions which provided, in relevant part, that: "(3) The probationer shall not access any internet services from any handheld device (e.g., Palm Pilots, Blackberries, and mobile telephones)"; and "(4) The probationer shall not use, enter, visit, participate in, or remain in any online chat room, bulletin board service, message board service, social networking site or service (for example, Facebook.com, Twitter.com, Instagram.com), or any other online communication service, with the sole exception of electronic mail." Id. at 704. The discussion during the plea colloquy clarified the scope of these two conditions such that, in summary, the third condition prohibited any Internet access from

handheld devices, and the fourth condition prohibited the use of social media on any device (except email). Id. at 705. When read together, the two conditions appeared to permit non-social-media Internet access (including email) from non-handheld devices. Id. While on probation, the defendant accessed "images of young girls wearing scanty dance costumes in provocative poses" and annotated print-outs of these materials by hand with the girls' names, ages, information about their siblings, and smiley faces in some cases. Id. at 706. He accessed these and similar materials using search engines (e.g., Google) and Wikipedia on computers, and emailed some of them to himself. Id. at 705. While acknowledging that the defendant's conduct was "troubling," the appeals court held that "the evidence was insufficient to permit the judge to find that he violated special condition four," because "[s]pecial condition four did not prohibit the defendant from using the Internet generally, or downloading information from it." Id. at 710 ("the defendant cannot be found in violation of probationary conditions that might have been intended or would have made sense, only those that are unambiguous and of which he has notice.").

In dicta, the King court wrote: "with the benefit of appellate hindsight, one cannot help but ask whether special condition four should not have been written differently and, in particular, whether it should have expressly prohibited the defendant from using a computer to access images or information about children, whether via the Internet or otherwise." Id. at 710. Further, "recogniz[ing] both the importance and difficulty of drafting clear special conditions of probation, especially when they involve technology," the court suggested it would "be helpful to supplement existing sources with a set of model, nonbinding special conditions" "for sex offenders and those who use technology to commit crimes," among others. Id. at 711.

Special conditions of probation that refer to pornography may use the "common meaning" of pornography, and may prohibit constitutionally protected activity that may not be the basis of an independent criminal conviction. Hamilton, 95 Mass. App. Ct. at 787.

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography,." Id. at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. Defendant argued that under Free Speech Coalition, which held facially unconstitutional a statute that criminalized possession of "sexually explicit images that appear[ed] to depict minors" but were actually "created by using adults who look like minors or by using computer imaging," Ashcroft v. Free Speech Coalition, 535 U.S. 234, 239–40 (2002), the explicit stories he posessed were not pornography because they were "'fantas[ies]' that [did] not involve actual children." Hamilton, 95 Mass. App. Ct. at 787. The court rejected defendant's argument, noting "that a probation condition is enforceable, even if it infringes on a defendant's ability to exercise constitutionally protected rights, so long as the condition is 'reasonably related' to the goals of sentencing and probation." Id. (quoting Commonwealth v. Lapointe, 435 Mass. 455, 459 (2001)). The court was not considering a facial challenge to a criminal statute, but rather had to decide the question of "whether a reasonable person in the defendant's circumstances would have known that the stories constitute

pornography in violation of his probation conditions." Id. Thus, "[t]he discussion in Free Speech Coalition [was] not germane to that question because the common meaning of pornography is not limited to materials depicting actual people. For example, had the defendant been found in possession of computer-generated images of what appeared to be children engaging in sexual activity, he indisputably would have been in violation of his probation, even though Free Speech Coalition says that those same images cannot be the basis of a criminal conviction." Hamilton, 95 Mass. App. Ct. at 787.

IV. Expert Testimony About Technology

Expert testimony is ordinarily required when the subject of the testimony "is beyond the common knowledge or understanding of the lay juror." Commonwealth v. Sands, 424 Mass. 184, 186 (1997). Even if a juror does not have personal experience of a technology, a lay juror, from common experience and knowledge, may understand the required concepts when provided sufficient non-expert testimony and evidence. Commonwealth v. Bundy, 465 Mass. 538, 546 (2013) (finding the victim's testimony and photographic evidence sufficient to keep jurors from engaging in conjecture about an Xbox and its accessories) (citing Commonwealth v. Sands, 424 Mass. 184, 186 (1997)).

- Commonwealth v. Javier, 481 Mass. 268 (2019). In this first-degree murder case, the defendant argued, among other things, that the trial judge erred in admitting opinion testimony by a cell phone company employee interpreting CSLI information. Id. at 269. The defendant argued that the employee, who was not an engineer, should not have been permitted to testify about how cell sites operate and how to locate a cell phone based on historical cell site information. Id. at 277, 285. The SJC noted that it had previously expressed some doubt—in an appeal by the defendant's co-venturer, see Commonwealth v. Gonzalez, 475 Mass. 396 (2016)—about the propriety of the phone employee's testimony in two respects. Javier, 481 Mass. at 286. In particular, the SJC explained in Gonzalez that the employee's testimony "'that calls are 'typically' transmitted through the closest cellular site, and that a call from [a particular] address was unlikely to have been transmitted through [a particular cell site] . . . may well have required a witness with greater technical expertise.'" Id. (quoting Gonzalez, 475 Mass. at 412 n.37). The Javier Court also noted, however, that the employee "properly qualified his testimony and explained that, even where a particular cellular telephone was most likely to connect to the nearest tower, there were many reasons why that might not happen," and therefore "the fact that he did not know or investigate the reasons why particular calls had connected to particular towers did not prejudice the defendant." Id. at 286. The SJC concluded that, "while it might have been better practice to exclude evidence that was of little assistance to the jury and that possibly could have been confusing, the judge did not abuse her discretion in allowing [the phone employee's] testimony about certain aspects of the CSLI." Id. at 286–87. Moreover, the portion of the employee's testimony "concerning the reasons that cellular telephones connect to cell towers, and what he 'expected' a particular telephone would be most likely to do here, would not have had any impact on the jury's verdict." Id. at 287.

- Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *3 (2016) (unpublished). In an appeal from convictions for possession and dissemination of child pornography claiming ineffectiveness of counsel for failure to object to the testimony of the Commonwealth's digital evidence analyst and to request a Daubert-Lanigan hearing to challenge the reliability and the admissibility of his testimony, the Appeals Court found the claim unfounded. Id. at *3. The prosecution's case was based on evidence found on the defendant's laptop. Id. at *1. The AGO analyst connected the laptop's hard drive to a "write blocker"—thus preventing any data additions or removals—and then created a duplicate image of the drive with a program called Encase. Id. A search of the duplicate image resulted in the discovery of three (3) peer-to-peer file sharing programs: "(1) LimeWire (containing more than 900 videos and images of child pornography); (2) eMule (containing more than 400 videos of child pornography); and (3) Ares (containing several search terms consistent with child pornography)." Id. at *1 The AGO analyst also examined the browsing history, text messages, and photographs on the laptop and the defendant's cell phone to corroborate his ownership and exclusive use of the two items. Id. The court found that the Commonwealth presented a strong case at trial and that "the defendant [did] little more than offer [u]nsupported speculation that further examination of the reliability and the admissibility of the prosecution's expert testimony would have undermined the prosecution's case." Id. at *3 (quotation and citation omitted).

V. List of Cases Organized by Device/Evidence Type

This section provides a quick reference list of the cases that appear elsewhere in this Guide, organized by device or evidence type. Case descriptions are in the respective sections where they are discussed.

A. Cell Phone Searches

- Riley v. California, 134 S. Ct. 2473 (2014).
- Commonwealth v. Barillas, 484 Mass. 250 (2020).
- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020).
- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019)

B. Search of Computer Files

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014).
- Commonwealth v. McDermott, 448 Mass. 750 (2007).
- Commonwealth v. Kaupp, 453 Mass. 102 (2009).
- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished).

C. Email

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

D. CSLI, GPS, and Other Location Technologies

- Carpenter v. United States, 138 S. Ct. 2206 (2018).
- United States v. Jones, 565 U.S. 400 (2012).
- Commonwealth v. Gosselin, 486 Mass. 256 (2020).
- Commonwealth v. Wilson, 486 Mass. 328 (2020)
- Commonwealth v. Davis, 97 Mass. App. Ct. 633 (2020).
- Commonwealth v. Wilkerson, 486 Mass. 159 (2020).
- Commonwealth v. McCarthy, 484 Mass. 493 (2020).
- Commonwealth v. Mora, 485 Mass. 360 (2020).
- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020).
- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020).
- Commonwealth v. Vasquez, 482 Mass. 850 (2019).
- Commonwealth v. Hobbs, 482 Mass. 538 (2019).
- Commonwealth v. Fredericq, 482 Mass. 70 (2019).
- Commonwealth v. Lugo, 482 Mass. 94 (2019).
- Commonwealth v. Almonor, 482 Mass. 35 (2019).
- Commonwealth v. Feliz, 481 Mass. 689 (2019).
- Commonwealth v. Johnson, 481 Mass. 710 (2019).
- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018).
- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017).
- Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016).
- Commonwealth v. Estabrook, 472 Mass. 852 (2015).
- Commonwealth v. Augustine, 467 Mass. 230 (2014).
- Commonwealth v. Collins, 470 Mass. 255 (2014).

E. Text Messages

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.).
- Commonwealth v. Fulgiam, 477 Mass. 20 (2017).

All Traffic Solutions Inc.
14201 Sullyfield Circle,
Ste 300
Chantilly, VA 20151
Phone: 814-237-9005
Fax: 814-237-9006
DUNS #: 001225114
Tax ID: 25-1887906
CAGE Code: 34FQ5

QUOTE Q-69272

DATE: 07/06/2022

Mail Purchase Orders to:
3100 Research Dr.
State College, PA
16801

Contract:

Questions contact:
MANUFACTURER:
All Traffic Solutions
Matthew O'Brien
(571) 321-5449
x 265
mobrien@alltrafficsolutions.com

Independent Sales Rep:

BILL TO:
Massachusetts State Police
50 Maple St
Milford MA 01757

Billing Contact:

SHIP TO:
Massachusetts State Police
50 Maple St
Milford MA 01757
Attn: Tyson DeLong

PAYMENT TERMS:
Net 30

CUSTOMER:
Massachusetts State Police

CONTACT:(508) 820-2284

ITEM NO:	DESCRIPTION:	QTY:	EACH:	EXT. PRICE:
4001774	Shield 12B with 11.5Ah, Integrated Solar, and charger	1	$3,145.00	$3,145.00
4000519	Traffic Data Collection; stores vehicle statistics locally for later analysis	1	$500.00	$500.00
4001763	Trailer, ATS-3, 90W solar panel included	1	$3,950.00	$3,950.00
4000754	USB cable, 16ft, extra long for trailer or pole	1	$32.00	$32.00
4000641	Shipping and Handling Common Carrier	1	$1,161.00	$1,161.00
4001190	Discount - New Purchase	1	($888.00)	($888.00)

Special Notes:

SALES AMOUNT: $7,900.00

TOTAL USD: $7,900.00

Duration: This quote is good for 60 days from date of issue.
Shipping Notes: All shipments shall be FOB shipper. Shipping charges shall be additional unless listed on quote.
Taxes: Taxes are not included in quote. Please provide a tax-exempt certificate or sales tax will be applied.
Warranty: Unless otherwise indicated, all products have a one year warranty from date of sale. Warranty extensions are a component of some applications that are available at time of purchase. A Finance Charge of 1.5% per month will be applied to overdue balances. GSA GS-07F-6092R

Authorization: By Signing below, I indicate that my organization does not require a purchase order and I am authorized to commit my organization to this order.

Signature: _____ Date: _____

Print Name: _____ Title: _____



MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MassDOT)
10 PARK PLAZA
BOSTON, MA 02116

REQUEST FOR RESPONSE (RFR)

Equipment, Parts & Services for Telecommunications, ITS, IPCS Systems

COMMBUYS Bid: BD-20-1030-0P100-0P070-49476
Project Info #: 111753

Date: Revised 9 July 2020

Rolling Enrollment: ***Bidders may submit qualifications response at anytime***

Please Note: This is a single document associated with a complete Bid (also referred to as Solicitation) that can be found on www.COMMBUYS.com. All Bidders are responsible for reviewing and adhering to all information, forms and requirements for the entire Bid, which are all incorporated into the Bid. Bidders may also contact the COMMBUYS Helpdesk at COMMBUYS@state.ma.us or the COMMBUYS Helpline at 1-888-MA-STATE. The Helpline is staffed from 8:00 AM to 5:00 PM Monday through Friday Eastern Standard or Daylight time, as applicable, except on federal, state and Suffolk county holidays.

1 RFR INTRODUCTION AND GENERAL DESCRIPTION

1.1 Procurement Scope and Description

The Massachusetts Department of Transportation (MassDOT) seeks vendors to provide specialized Equipment, Parts & Services for MassDOT's Transportation and Roadway Telecommunications, Intelligent Traffic systems (ITS), Integrated Project Control Systems (IPCS).

1.2 Background Information

MassDOT operates a wide array of transportation systems throughout the Commonwealth, many of which are integrated with Federal and neighboring states. Key Telecommunications, ITS, IPCS Systems are in place to keep these systems running efficiently, providing a safe system for all users. MassDOT seeks to place pre-qualified vendors under Master Service Agreement contracts to supply equipment, parts, and services for the systems in place as well as replacement systems potentially needed in future years, within the terms of this solicitation. See Section 3.0 below.

NOTE: MassDOT monitors closely products and vendors available through statewide contracts managed by the Operational Services Division (OSD)[1]. MassDOT does not seek to replace product or vendors currently available through OSD statewide contracts by this solicitation.

1.3 Applicable Procurement Law

This Bid is issued under the following laws: MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00

1.4 Number of awards

MassDOT intends to make a **MULTIPLE** awards.

1.5 Adding Contractors after Initial Contract Award

If, over the life of the Contract, MassDOT determines that additional contractors should be added, these may be drawn from qualified companies which responded to this solicitation but were not awarded contracts. If necessary to meet the needs of MassDOT, the solicitation may be reopened to obtain additional responses from interested vendors

1.6 Eligible Entities

~~Any contract resulting from this Bid will be open for use by **MassDOT only.**~~

Any contracts resulting from this RFR may be used by **all departments of MassDOT**, the Commonwealth, including all constitutional offices, the legislature, and the judiciary; cities, towns, municipalities, counties, and other political subdivisions of the Commonwealth, including schools, and other service districts; authorities, commissions, institutions of higher education, and quasi-public agencies, and Not for Profit contractors currently contracting with the Commonwealth to provide human and social services; and other eligible entities designated in writing by the State Purchasing Agent. All entities other than MassDOT must execute a separate contract that meets their own legal and business requirements.

[1] https://www.mass.gov/service-details/find-a-statewide-contract-user-guide

THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

OFFICE OF THE ATTORNEY GENERAL
ATTORNEY GENERAL MAURA HEALEY



A PROJECT OF THE CRIMINAL BUREAU
DIGITAL EVIDENCE LABORATORY
APPEALS DIVISION

JUNE 2021

A NOTE TO READERS OF THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

The Massachusetts Digital Evidence Guide (hereinafter "Guide") is only to be used as an educational resource. This Guide is not legal advice. The purpose of this Guide is to provide the reader with an understanding of the Massachusetts statutes and cases impacting criminal investigations and prosecutions that involve technology or digital evidence. This Guide, and its provisions, are not policy. This Guide does not suggest modifying or replacing any existing agency practices or procedure(s). Readers should consult with appropriate authorities, prosecutors, or legal counsel for necessary legal advice, case or statutory interpretation, or implementation of the document for any internal use. Readers who intend to rely on cases and statutes cited in this Guide should consult with the source document, confirm the interpretation, and investigate subsequent history. Questions or comments about, or suggestions for this Guide can be e-mailed to agodel@mass.gov.

THE MASSACHUSETTS DIGITAL EVIDENCE GUIDE

Office of the Attorney General, Maura Healey

Contents

Contents 2

I. Investigation 7

A. The Search and Seizure of Digital Evidence 7

1. Was There a Search or Seizure? 7

a) Searches and the Reasonable Expectation of Privacy 8

(1) Standing 8

(2) One Party Consent 9

(3) The Third-Party Doctrine 9

(4) Surveillance in Public: Public View Principle, Mosaic Theory, and More 13

(5) Peer-to-Peer and Other Network File Sharing 14

(6) Expectation of Privacy in Data That Is Not One's Own 16

(7) Probationers, Parolees, and Court-Ordered Monitoring 17

b) Seizures and Interference with Possessory Interest 19

c) Private Party Searches 20

(1) Initial Search Made by Private Party 20

(2) Warrantless Search: Private Citizen or State Actor 21

(3) An ISP's Reporting Obligation Does Not Make it a State Agent 22

2. Was a Search or Seizure Reasonable? 22

a) Warrants 22

(1) Probable Cause / Affidavit 23

(2) Independent Source Doctrine 30

(3) Particularity / Scope 31

(4) Staleness of Information Supporting Probable Cause 36

(5) Timely Execution of the Warrant 38

(6) Manner of Executing the Warrant 39

b) Exceptions to the Warrant Requirement 40

(1) Search Incident to Arrest 40

(2) The Plain View Doctrine 42

(3) Exigent Circumstances 44

(4) Emergency Aid Exception 45

(5) Inventory Exception 46

(6) Consent 47

3. The Exclusionary Rule 48

a) Good Faith / Substantial and Prejudicial 48

b) Inevitable Discovery 49

B. Search of Electronic Service Providers 49

1. General Overview of Stored Communications Act 49

2. Search warrants served on out-of-state Internet service providers 50

C. Encryption and Self Incrimination 50

1. The Foregone Conclusion Doctrine 50

2. Encryption 51

3. Sample Decryption Protocol 54

D. Searches Implicating Attorney-Client Privilege 54

1. Post-Indictment Email and File Searches 55

2. Taint Teams 55
3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails) 56
II. Evidentiary Matters 57
A. Judicial Discretion 57
1. Trial Judge's Discretion 57
2. Demonstrative Photographs 57
B. Discovery 57
1. Pornographic Images in Child Pornography Cases 57
2. Wiretap transcripts 58
3. Cell phone data 58
C. Authentication 59
1. Generally 59
2. Photographs and Digital Images, Videos, and CDs 59
3. Digitally Enhanced Images and Video 60
4. Transcripts of Recordings 60
5. Email 61
6. Chatrooms 62
7. Text Messages 62
8. Information Available on Websites and Social Networks 62
9. Software Programs Used in Investigation 64
10. GPS and Probation 64
D. Technological evidence as the basis of criminal conviction 65
E. Best Evidence Rule 66
1. Best Evidence Rule - Generally 66
2. Digital Images 66

3. Admission of Duplicate Evidence 66
4. Videos 67
5. Email 67
6. Summaries 67
F. Hearsay 68
G. Business Records Exception 68
1. Email 68
2. Computer Records 69
H. Confrontation Clause 69
1. Software-generated information 69
2. Secondary Examiners 70
III. Cybercrimes 72
A. Possession of Child Pornography 72
1. Multiple Convictions Require Multiple "Caches" 72
2. Brief Possession is Sufficient 72
3. Receipt by Cell Phone is Sufficient 73
4. Malware and Computer Viruses Defense 73
5. Probable cause / Staleness in Child Pornography Cases 73
B. Statutory Terms of Mass Gen. Laws ch. 272 74
1. "Dissemination" 74
2. Computer "Depictions" 74
3. Child Enticement 75
4. "Visual Material" 75
5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31 75
6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A 75

7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A 76
8. Lewdness 77
C. Special Conditions of Probation 77
IV. Expert Testimony About Technology 79
V. List of Cases Organized by Device/Evidence Type 80
A. Cell Phone Searches 80
B. Search of Computer Files 80
C. Email 80
D. CSLI, GPS, and Other Location Technologies 81
E. Text Messages 81

I. Investigation

A. The Search and Seizure of Digital Evidence

As with physical evidence, searches and seizures of digital evidence must be reasonable to be valid. This section provides a summary of Fourth Amendment law as it relates to the search and seizure of digital evidence. It also references Article Fourteen of the Massachusetts Declaration of Rights, which parallels the Fourth Amendment, but is sometimes more expansive.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Article Fourteen (art. 14) of the Massachusetts Declaration of Rights is similar to the Fourth Amendment, but since 1985, the Supreme Judicial Court ("SJC") has interpreted it as providing broader protections than its federal counterpart. Commonwealth v. Upton, 394 Mass. 363, 373 (1985) ("We conclude that art. 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause.").

To determine whether law enforcement action constitutes an unreasonable search or seizure, courts ask two questions. First, was the action a search or seizure within the meaning of the Fourth Amendment? E.g., Commonwealth v. Magri, 462 Mass. 360, 366 (2012) ("In deciding whether police conduct violates the Fourth Amendment or art. 14 of the Massachusetts Declaration of Rights, we first determine whether a search, in the constitutional sense, has taken place."). Second, was that search or seizure reasonable? See, e.g., Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness." (internal quotation marks omitted)).

1. Was There a Search or Seizure?

"A search implicating the Fourth Amendment occurs 'when an expectation of privacy that society is prepared to consider reasonable is infringed' and a seizure of property for purposes of the Fourth Amendment occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'" Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (quoting United States v. Karo, 468 U.S. 705, 712 (1984)) (finding installation and use of a GPS tracking device on a car to be a seizure under Massachusetts art. 14 because it requires entering the vehicle and using the electricity of the defendant's car).

a) Searches and the Reasonable Expectation of Privacy

For a search to implicate the Fourth Amendment, the defendant must have a "reasonable expectation of privacy" in the place to be searched. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); see also United States v. Heckencamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding a college student had a reasonable expectation of privacy in the contents of his personal computer because it was located in his dorm room, was protected by a password, and was not subject to regular university monitoring). A person's expectation of privacy is reasonable "if he can demonstrate a subjective expectation that his activities would be private, and he can show that his expectation was one that society is prepared to recognize as reasonable." Heckencamp, 482 F.3d at 1146 (internal quotation marks, brackets, and citations omitted). Individuals generally have a reasonable expectation of privacy in their personal computers and files. See id. at 1146–47 (listing cases to that effect). In Heckencamp, "[t]he salient question [was] whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network." Id. at 1146.

When challenging the constitutionality of a search, the defendant bears the initial burden of establishing that a search occurred. See Commonwealth v. D'Onofrio, 396 Mass. 711, 714-15 (1986); Commonwealth v. Alvarez, 480 Mass. 1017, 1018 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer).

The sections below explore the contours of the reasonable expectation of privacy, discussing: (1) standing; (2) one-party consent; (3) the third-party doctrine; (4) surveillance in public; (5) file sharing over networks; (6) reasonable expectations of privacy in data that is not one's own; and (7) diminished privacy expectations in the context of probationers, parolees, and court-ordered monitoring.

(1) Standing

Standing to challenge a warrantless search or seizure may be in question when the location or item searched or seized does not belong to the challenging party.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully suppressed CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105, 107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Commonwealth v. Almonor, 482 Mass. 35 (2019), the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Almonor, 482 Mass. at 47-48 (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The Court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have

automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because, "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Id. at 108. The Court found that the defendant did have standing to challenge the search of his own cell phone, but the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 108-09.

(2) One Party Consent

In Massachusetts, "one party consent" does not negate a reasonable expectation of privacy of the non-consenting party. While the Supreme Court held that warrantless electronic surveillance with "one party consent" does not implicate the Fourth Amendment, United States v. White, 401 U.S. 745, 751 (1971), the SJC found such surveillance impermissible under art. 14 of the Massachusetts Declaration of Rights, Commonwealth v. Blood, 400 Mass. 61, 70 (1987). Because it found there is a reasonable expectation of privacy in conversations that occur among "a narrow compass of known listeners" in private homes, the SJC concluded that the warrantless electronic surveillance was a violation of that constitutional provision. Id. Accordingly, "one party consent" did not obviate the need for a warrant under art. 14. Id.

(3) The Third-Party Doctrine

In United States v. Miller, 425 U.S. 435 (1976), and Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court articulated what has become known as the "third-party doctrine." Under this doctrine, "the Fourth Amendment does not prohibit the obtaining of information revealed [by a suspect] to a third party and conveyed by him to Government authorities," regardless of the suspect's expectation of how the information might be used. Miller, 425 U.S. at 443. Massachusetts has traditionally followed the Supreme Court's guidance on the third-party doctrine. See, e.g., Commonwealth v. Cote, 407 Mass. 827, 833–36 (1990) (holding that a defendant had no reasonable expectation of privacy in telephone message records held by a third-party answering service for the reasons cited in Miller).

- United States v. Jones, 565 U.S. 400 (2012). Unanimous decision holding that a Fourth Amendment "search" occurs where law enforcement places a GPS device on defendant's car. Id. at 411. The Court's opinion, authored by Justice Scalia, focused on the Government's intrusion on the defendant's physical property and applied "an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted." Id. In contrast, Justice Sotomayor's concurrence in Jones emphasized that "the Fourth Amendment is not concerned only with trespassory intrusions on property," id. at 954, and brought the issues later addressed by Carpenter v. United States, 138 S. Ct. 2206 (2018), to the forefront, see Jones, 565 U.S at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age…").

Carpenter v. United States, 138 S. Ct. 2206 (2018) and Commonwealth v. Augustine, 467 Mass. 230 (2014) modified the third-party doctrine for at least one specific type of information—cell site location information ("CSLI"). The holding of Carpenter is that law enforcement effects a Fourth Amendment "search" by obtaining at least one week's worth of a defendant's CSLI from a third-party cellular provider. See Carpenter, 138 S. Ct. 2206, 2217 n.3. The comparable holding from Augustine is that subpoenaing two weeks' of CSLI information is a "search." See Augustine, 467 Mass. 230, 233, 255 (2014).

- Carpenter v. United States, 138 S. Ct. 2206 (2018). The Government successfully applied for two court orders directing Carpenter's wireless carriers to disclose Carpenter's CSLI for select time periods within a four-month span. 138 S. Ct. at 2212. The first order sought 152 days of CSLI from MetroPCS, and the second order sought seven days of CSLI from Sprint. Id. Based in part off the information the Government acquired from Carpenter's CSLI, the Government charged Carpenter with six counts of robbery and six counts of carrying a firearm during a federal crime of violence. Id.

  The Supreme Court held that the Government's acquisition of Carpenter's CSLI was a search of Carpenter that required a warrant supported by probable cause even though the Government acquired the CSLI from third-party wireless carriers. Id. at 2221. The Court declined to apply an expansive version of the third-party doctrine to CSLI partly because the data can reveal immense amounts of intimate information about who a suspect has been associating with and where a suspect has been travelling. Id. at 2219 ("There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today."). Furthermore, because cell phones are a nearly ubiquitous part of daily life and virtually every activity on a phone generates CSLI, the Court rejected the claim that Carpenter voluntarily disclosed his CSLI to his wireless carriers. Id. at 2220 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term.").

  While the Court stated that its ruling was "a narrow one" that applied only to CSLI, id., the dissents argued that the decision will have far-reaching consequences, e.g., Carpenter, at 2234 (Kennedy, J., dissenting) ("The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties."); see also id. at 2262 (Gorsuch, J., dissenting) ("Today the Court suggests that Smith and Miller distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to 'extend' those decisions to particular classes of information, depending on their sensitivity." (emphasis in original)); cf. Commonwealth v. Augustine, 467 Mass. 230, 253 (2014) (holding that although "we do not reject categorically the third-party doctrine," some forms of electronic evidence require "a different approach"). Given Americans' increasing dependence on technological devices that generate large amounts of personal data, it is possible that the Supreme Court's reasoning in Carpenter will someday result in a larger overhaul of the third-party doctrine.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case similar to Hobbs, considering retroactive application of Augustine's warrant requirement for CSLI data, the SJC again held constitutional a pre-Augustine CSLI request because the associated 18 U.S.C. § 2703 application satisfied the requisite probable cause standard. Id. at 166-72.

- Commonwealth v. Almonor, 482 Mass. 35 (2019). This case concerned an issue of first impression involving whether police action that causes an individual's cell phone to transmit its real-time location information violates any reasonable expectation of privacy. Id. at 41. Neither the Supreme Court's decision in Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018) nor the SJC's decision in Commonwealth v. Augustine, 467 Mass. 230, 4 N.E.3d 846 (2014) addressed this precise issue. The Commonwealth charged the defendant with murder after he shot and killed an individual and subsequently fled the scene of the crime. After a witness gave them the defendant's phone number, the police filed a "mandatory information for exigent circumstance requests" form with the telephone service provider. The telephone service provider "pinged" the defendant's phone and revealed the defendant's GPS coordinates to the police. Id. at 38-39. The Court granted the defendant's motion to suppress the warrantless "pinging." Id. The SJC reversed, holding that the warrantless pinging of the defendant's phone constituted a search under the Article 14 of the Massachusetts constitution, but that the warrantless search was justified by exigent circumstances, namely that the defendant was at large and believed to be armed and dangerous. It noted that searches occur when the government intrudes on a person's reasonable expectation of privacy and concluded that the defendant had a reasonable expectation of privacy in his cellular location data. Id. at 43-44. The Court held that real-time location data serves as a "proxy for the real-time location of the individual" because "cell phones are an indispensable part of daily life and exist as almost permanent attachments to their users' bodies." Id. at 45 (internal quotations omitted).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). In 2011, the government received historical CSLI from defendant's cell service provider pursuant to a 18 U.S.C. § 2703 order, without a warrant — well before 2014, when Augustine first articulated the warrant requirement for historical CSLI requests. Id. at 542-44. The SJC held that the government could "still satisfy the warrant requirement if it can establish that its 'application for the § 2703[] order met the requisite probable cause standard of art. 14,'" i.e., the same probable cause standard required of an affidavit in support of a search warrant for historical CSLI. Id. at 544 (quoting Augustine, 467 Mass. at 256). (This also comports with Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016), an earlier case considering retroactive application of Augustine to CSLI data obtained pre-Augustine pursuant to an 18 U.S.C. § 2703 order.)

- Commonwealth v. Fulgiam, 477 Mass. 20 (2017). In Fulgiam, the Commonwealth obtained recent text messages of the defendant pursuant to § 2703(a) of the Federal Stored Communications Act. Id. at 28; 18 U.S.C. § 2703(a) (2012). The Court held, on federal statutory and state constitutional grounds, that law enforcement required a warrant to obtain the text messages. See 477 Mass. at 31. An individual under Massachusetts state law has a "reasonable expectation of privacy in his text messages." Id. at 33. The third-party doctrine did not require

otherwise because "the nature of cellular telephone technology . . . [and] use in our current society render the third-party doctrine inapposite" in this context. Id. at 34.

- Commonwealth v. Estabrook, 472 Mass. 852 (2015). The SJC considered a request for CSLI and concluded that a defendant's reasonable expectation of privacy under art. 14 of the Massachusetts Declaration of Rights is not violated by a warrantless request for production of up to six (6) hours of historical CSLI. Id. at 854. It also established that the relevant consideration in determining the reasonable expectation of privacy is the length of time for which CSLI data is requested, not the time span ultimately sought to be introduced at trial. Id. at 858–59.

- Commonwealth v. Augustine, 467 Mass. 230 (2014). Police investigating a murder obtained the defendant's CSLI from his service provider pursuant to a 18 U.S.C. § 2703(d) order. Id. at 233. These orders are not warrants, so they cannot be used to effectuate a search for information protected by the Fourth Amendment or art. 14. The CSLI obtained helped police determine the defendant's location over the period they were investigating. See id. at 233–34. The Court considered but ultimately rejected the Commonwealth's argument that the third-party doctrine negated any reasonable expectation of privacy the defendant had in his CSLI. Id. at 241–56. It reasoned that art. 14 does not protect information voluntarily and intentionally transmitted to third parties (like the number dialed to initiate a call) but it does protect information incidentally transmitted (like the location information the cell phone provider acquires as a result of cell phone technology). Id. at 249–52. The Court found that the defendant therefore had a reasonable expectation of privacy in his CSLI, which, under art. 14, means that "the government must obtain a search warrant to obtain it." Id. at 252.

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). Law enforcement obtained thousands of emails related to fraudulent marketing claims from the defendant's Internet Service Provider (ISP). Id. at 281. The defendant challenged such access to his email on Fourth Amendment grounds. Id. at 282. The Sixth Circuit agreed and held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" Id. at 288 (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)). In finding that a reasonable expectation of privacy existed in this case, the Sixth Circuit analogized email transmitted via ISP to the contents of telephone conversations and closed letters, each of which received Fourth Amendment protection. See id. at 286–87. Rebutting the third-party doctrine argument, the Sixth Circuit—similar to the SJC in Augustine above—noted that the ISP in this case was an *intermediary* rather than the intended target of a conversation. Id. at 288. Thus, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." Id. Though binding only in the Sixth Circuit, this case has been cited by some of the largest email providers in requiring warrants to obtain the contents of email. See Brendan Sasso, *Facebook, email providers say they require warrants for private data seizures*, The Hill (Jan. 25, 2013), http://thehill.com/policy/technology/279441-facebook-email-providers-require-warrant-for-private-data. The Department of Justice also requires its prosecutors nationwide to follow this holding.

(4) Surveillance in Public: Public View Principle, Mosaic Theory, and More

Under the "public view" principle, individuals generally do not have a reasonable expectation of privacy in items or places that they expose to the public. California v. Ciraolo, 476 U.S. 207, 213 (1986) ("[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares"). In particular, "the government, without… a warrant, may use electronic devices to monitor an individual's movements in public to the extent that the same result could be achieved through visual surveillance." Augustine, 467 Mass. at 252. (Note that this principle as stated in Augustine is in some tension with the SJC's decision in Mora, as discussed below.)

Courts have limited the public view principle in "constitutionally sensitive" settings (epitomized by the home) where individuals have a strong expectation of privacy that society is prepared to recognize, especially where technology has enabled previously infeasible collection of information about the inside of a home via surveillance technology situated outside the home (i.e., in public). See Kyllo v. United States, 533 U.S. 27 (2001) (holding warrantless surveillance of heat levels inside a home using thermal-imaging equipment outside the home to be an unconstitutional search).

Recent developments suggest that courts are increasingly recognizing constitutional warrant requirements in more situations involving surveillance in public places, when such surveillance is particularly expansive and detailed, or implicates "constitutionally sensitive" domains such as the home. The SJC has recognized the "mosaic theory" or "aggregation principle for the technological surveillance of public conduct," under which "'the cumulative nature of… information collected [when collected over a long enough period] implicates a privacy interest on the part of the individual who is the target of the tracking,'" even when the individual activities or data points surveilled would not enjoy constitutional protection taken alone. Commonwealth v. McCarthy, 484 Mass.493, 503-04 (2020)(quoting Augustine, 467 Mass. at 253); see also Jones, 565 U.S. at 416 (Sotomayor, J., concurring).

- Commonwealth v. McCarthy, 484 Mass. 493 (2020). The Court considered the constitutionality of warrantless use of automatic license plate readers (ALPRs), which are "cameras combined with software that allows them to identify and 'read' license plates on passing vehicles." Id. at 494. Drawing on the "mosaic theory," the SJC stated that "[a] detailed account of a person's movements, drawn from electronic surveillance, encroaches upon a person's reasonable expectation of privacy because the whole reveals far more than the sum of the parts," and noted that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes." Id. at 504, 506. On the facts of the case, however, the SJC found no constitutional violation: "[T]he analysis should focus, ultimately, on the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance [at issue]. … [F]or this case, we consider the constitutional import of four cameras placed at two fixed locations… [and] conclude that the limited use of ALPRs in this case does not constitute a search within the meaning of either art. 14 or the Fourth Amendment." Id. at 506, 508,509.

Pole camera surveillance is a notable area where courts' approaches in applying the "public view" principle have been shifting recently, especially after Carpenter, 138 S. Ct. 2206, and Jones, 565 U.S. 400. While "[m]ost courts to have addressed pole camera surveillance have concluded that it does not infringe on any reasonable expectation of privacy" under the "public view" principle, "several courts have reassessed prolonged pole camera surveillance." Commonwealth v. Mora, 485 Mass. 360, 364-65 (2020) (citing as examples United States v. Vargas, No. CR-13-6025 (E.D. Wash. Dec. 15, 2014) (six weeks of pole camera surveillance was search); State v. Jones, 2017 S.D. 59 (2017) (two months was search); People v. Tafoya, 2019 COA 176 (Colo. App. 2019) (three months was search)). Mora is the most recent Massachusetts case on pole camera surveillance.

- Commonwealth v. Mora, 485 Mass. 360 (2020). Investigators installed pole cameras on public telephone and electric poles for the purpose of surveilling the defendants. Id. at 361. Most of the cameras were aimed at the homes of defendants or other individuals; one was aimed at a street that a defendant used to conduct his drug business. Id. at 362. The cameras had video but not audio recording capabilities, they could not view inside any residence, and they did not have infrared or night vision capabilities; however, investigators could remotely zoom and angle the cameras in real time. Id. The footage was stored in a searchable format that allowed officers to review previously-recorded events. Id. The SJC held that the pole camera surveillance of the defendants' homes was a warrantless search in violation of Article 14 of the Massachusetts Constitution. Id. at 370-76. Pole camera surveillance of public streets frequented by the defendants away from their homes was not subject to a warrant requirement, however, as defendants had no reasonable expectation of privacy in those locations. Id. at 369. The defendants' homes did not have fencing or other attempts to shield the residences from view, a fact that the court held immaterial to the constitutionality of surveillance. Id. at 366-67. The court noted that the Fourth Amendment might well require the same outcome, but declined to reach the federal constitutional question as the case could be resolved on state constitutional grounds. Id. at 361.

(5) Peer-to-Peer and Other Network File Sharing

The following cases illustrate when making data accessible to the public or certain networks via peer-to-peer file sharing techniques eliminates one's reasonable expectation of privacy.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Defendant was an instructor at a high school's electronics shop. Police officers remotely observed pirated movies and child pornography in an open share folder of a computer named Joester7437, which was connected to the school's network. Id. at 103–05. [Note: Joester7437 was later determined to belong to a student. Id. at 105.] While searching the school for Joester7437, the police found a computer/server named "Nightcrawler." Id. at 105. Nightcrawler's screen displayed an open share folder with the same pirated movie as was found on Joester7437. Id. "The source of the open share was Sinister, another unauthorized computer logged onto the high school's network." Id. The police found Sinister in the defendant's office, but that computer was password protected. Id. They seized Sinister "on probable cause to believe that it contained child pornography and copyrighted intellectual property." Id. They then received a search warrant for it based on an affidavit

alleging: (1) both shared folders (in Joester7437 and Sinister) had a copy of the same pirated movie, (2) Joester7437's open share folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 111. The defendant did not dispute that he had no reasonable expectation of privacy in files shared with the network. Id. at 107. Instead, the defendant argued that he did have a reasonable expectation of privacy in his *private* files and that there was no probable cause to search the private files for child pornography. Id. The Court held that the affidavit in support of the search warrant did not establish probable cause to believe that child pornography was located in the private files on the defendant's computer (Sinister). Id. at 111. The SJC noted: "None of these facts, even when considered together, provided a 'substantial basis' to believe that the defendant's private files contained child pornography." Id.

- Commonwealth v. Hay, 90 Mass. App. Ct. 1122 (2016) (unpublished). Defendant argued that the pre-warrant investigation was a "search" within the Fourth Amendment because the P2P [peer-to-peer] network was open only to a small group of known individuals, id. at *6, and because law enforcement used specialized SHA technology to identify a file on the defendant's computer that was likely to contain child pornography, id. at *7 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001) (government's use of device not in general public use "to explore details of the home that would previously have been unknowable without physical intrusion" is a search)). The appeals court held that, though it is possible that a file-sharing network open only to a small group of known individuals might give rise to a reasonable expectation of privacy in the files, the defendant had not argued or shown that the network in question here (Gnutella), as used with the specific software client used by the defendant (LimeWire), was such a network. Id. at *7. The appeals court also held the investigation was not a search because the defendant offered no evidence that the SHA technology enabled law enforcement to learn any more about the files than could any other P2P user. Id.

- United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010). Defendant shared child pornography over a peer-to-peer file sharing network that was being monitored by police using special forensic software. Id. at 1046–47. Police remotely downloaded the incriminating files from the defendant's folder on the peer-to-peer network. Id. at 1047. The Ninth Circuit held the defendant had no reasonable expectation of privacy in files that anyone who had access to the network could download. See id. at 1048. The court ruled this way notwithstanding the defendant's attempts to keep the files private because even though his subjective intent demonstrated a desire for privacy, it would be objectively unreasonable to uphold an expectation of privacy "in the face of such widespread public access." Id. The court also rejected the defendant's argument that the special forensic software used by investigators constituted a search. It cited several other cases supporting the proposition that special tools could be used to access already-public information, like the files in this case, because public information enjoys no Fourth Amendment protections. See id. at 1048.

- United States v. King, 509 F.3d 1338 (11th Cir. 2007). Defendant had child pornography on a personal computer connected to a military base network. Id. at 1339. His "files were 'shared' over

the entire base network," id. at 1342, and an airman searching the network remotely downloaded those files, id. at 1340–41. The defendant took several steps—ultimately unsuccessful—that he believed shielded his hard drive from access by others. Id. at 1341. Even though the defendant manifested a subjective expectation of privacy by attempting to secure the files, id., the court found that his failure to actually secure the files rendered that expectation objectively unreasonable, id. at 1342. In reaching this conclusion, the court analogized to a prior case holding that a defendant had no objectively reasonable expectation of privacy in the unsecured common area of a multi-unit apartment building. Id. In both cases, the fact of public access rendered any subjective expectation of privacy objectively unreasonable. Id.

- United States v. Ladeau, No. 09–40021–FDS, 2010 WL 1427523 (D. Mass. April 7, 2010). Defendant shared child pornography over a secured peer-to-peer network that allowed him to select who could download his files. Id. at *1. He allowed downloads by a private user who then turned his account over to the Royal Canadian Mounted Police. Id. The court held that even though the defendant manifested a subjective expectation of privacy through his actions, this expectation was not objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at *4. "No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access." Id. So, "[o]nce Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable." Id. at *5.

- United States v. Thomas, Nos. 5:12–cr–37, 5:12–cr–44, 5:12–cr–97, 2013 WL 6000484 (D. Vt. Nov. 8, 2013). Defendants in this case shared child pornography over peer-to-peer networks. Id. at *17. Police found the defendants by using automated scanning tools designed to detect child pornography shared on peer-to-peer networks. Id. After a lengthy explanation of file sharing, hash values, and investigative software and testing tools, id. at *2–6, the court held that the defendants had no reasonable expectation of privacy in files they shared publicly on a peer-to-peer network, id. at *19–20. In making this ruling, the court relied on United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010), along with other circuit cases. Id. at *19. The defendants argued against the inclusion of partially downloaded files in the evidence used against them, saying they would not have shared those files once the download was complete, but the court rejected this argument because those files were nonetheless being shared when the police searched and were therefore publicly accessible. Id. at *17. [Note: This case contains clear and thorough explanations of peer-to-peer networks, hash values, and TLO's CPS suite of tools.]

(6) Expectation of Privacy in Data That Is Not One's Own

The following cases address claims of a reasonable expectation of privacy in data that, in some sense, is not the movant's.

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to

challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable expectation of privacy in his movements. Id. at 77.

- Commonwealth v. Lugo, 482 Mass. 94 (2019). The court found that a juvenile defendant had no standing to challenge the "pinging" of another juvenile's cell phone in a second-degree murder case involving a botched robbery. Id. at 105,107-08. After determining that the "pinging" of the defendant's and his cohort's cell phones were searches under Almonor, the SJC turned to the question of whether the defendant had standing to challenge those searches. Lugo, 482 Mass. at 107; see Commonwealth v. Almonor, 482 Mass. 35, 47-48 (2019) (causing a cell phone to reveal its real-time location constitutes a search under Article 14). The Court held that without a possessory interest in the other juvenile's cell phone, the defendant did not have automatic standing to contest the search. Lugo, 482 Mass. at 107. Further, he did not have actual standing because "[a]lthough the defendant was with [the other juvenile] when her location was searched, the period of the search—less than two hours—was not sufficiently significant to allow the defendant standing." Lugo, 482 Mass. at 108. During the investigation, police became concerned that a second juvenile involved in the murder-robbery might be in danger, and contacted that individual's cell phone service provider, obtaining location data, and the names and numbers from recent calls. Id. at 106. Among these was the defendant's phone number, which police also "pinged," showing that he was at his residence with the second juvenile. Id. Police obtained a search warrant for the residence and "discovered evidence linking the defendant to the killing, including the murder weapon." Id. The SJC pointed out that, even if there had been no standing issue, the circumstances of police investigating a homicide and concerned for the cell phone user's safety would have rendered the defendant's challenge futile under the emergency aid exception. Id. at 108. The Court also held that, while the defendant had standing to challenge the search of his own cell phone, the information gathered from that search—the location of his residence—had already been gathered by other means, so no evidence came from the search. Id. at 109.

- Commonwealth v. Bryant, 447 Mass. 494 (2006). Law enforcement seized the "main file server" of a law firm pursuant to a warrant. See Commonwealth's Brief, 2005 WL 4062684, at *10 (Dec. 2005). The defendant, an employee of the firm, moved to suppress files he had worked on. See Bryant, 447 Mass. at 495. Denying the motion to suppress, the Supreme Judicial Court held that the defendant did not have a "reasonable expectation of privacy" in the firm's files and therefore did "not establish[] that he ha[d] standing to challenge the seizure of the files." See id. at 497.

(7) Probationers, Parolees, and Court-Ordered Monitoring

Probationers subject to court-ordered monitoring have a diminished expectation of privacy.

- Commonwealth v. Feliz, 481 Mass. 689 (2019) (decided on the same day as Commonwealth v. Johnson, 481 Mass. 710 (2019), infra). The SJC held that Mass. Gen. Laws ch. 256, § 47, which mandates GPS monitoring as a condition of probation in connection with most sex offense convictions, is "overinclusive" because "GPS monitoring will not necessarily constitute a

reasonable search for all individuals convicted of a qualifying sex offense." Id. at *1; Mass. Gen. Laws ch. 256, § 47 (2018). The Court held that, under Article 14 of the Massachusetts Declaration of Rights, an individualized determination of reasonableness is required for any search that is "more than minimally invasive," and "GPS monitoring is not a minimally invasive search." 2019 WL at *7. Thus, a judge must "conduct a balancing test that weighs the Commonwealth's need to impose GPS monitoring against the privacy invasion occasioned by such monitoring." Id. at *1. Whether the monitoring is determined to be reasonable "depends on a constellation of factors," and "no one factor will be dispositive in every case." Id. at *8. The fact that a probationer accedes to a contract of probation that requires GPS monitoring or signs a GPS equipment contract does not constitute consent that waives the probationer's Article 14 rights. Id. at *8. With respect to Mr. Feliz, the SJC held that "the Commonwealth's particularized reasons for imposing GPS monitoring . . . do not outweigh the privacy intrusion occasioned by the requirement of GPS monitoring." Id. at *8; accord id. at *10–13. In support of that conclusion, the Court noted that the defendant "was convicted of noncontact sex offenses," and that the Commonwealth "ha[d] not presented evidence sufficient to indicate that th[e] defendant pose[d] a threat of reoffending or otherwise violating the terms of his probation." Id. at *10.

- Commonwealth v. Johnson, 481 Mass. 710 (2019) (decided on the same day as Commonwealth v. Feliz, supra). At defendant's trial for breaking and entering and larceny, the Commonwealth introduced GPS location data recorded from a GPS monitoring device that the defendant was wearing as a condition of probation. Id. at *1. The historical GPS data had been retrieved and reviewed without a warrant after the defendant's probation was completed. Id. at *2–3, *6. Defendant argued that the trial court erred in admitting the GPS location data at trial. Id. at *3. The SJC held that (1) the original imposition of GPS monitoring as a condition of defendant's probation was a search, but it was reasonable "in light of the defendant's extensive criminal history and willingness to recidivate while on probation"; and (2) no subsequent search occurred because, "once the GPS device was attached to the defendant, he did not possess a reasonable expectation of privacy in data targeted by police to determine his whereabouts at the times and locations of suspected criminal activity that occurred during the probationary period." Id. at *1. The SJC noted that the police had conducted a narrow analysis to determine whether the defendant was present at times and places where crimes had been committed, and that a broader "indiscriminate rummaging" through months of GPS data "might raise different, more difficult constitutional questions about objective expectations of privacy, even for a probationer subjected to GPS monitoring." Id. at *10.

- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017). Police investigating a robbery "mapped" the location of a defendant wearing a GPS monitoring device while out on bail for a domestic violence offense. See id. at 298. This process revealed that the defendant was near the scene of the robbery at the time of the break-in. See id. The Commonwealth introduced the GPS evidence at trial and the defendant was convicted. Id. at 296–97. The Massachusetts Appeals Court affirmed, rejecting defendant's argument that he—subject to court ordered monitoring—retained a reasonable expectation of privacy in his movements and thus was subject to a Fourth Amendment "search". See id. at 306.

Parolees have a diminished expectation of privacy—lower even than that of probationers—both under the Fourth Amendment, Samson v. California, 547 U.S. 843, 850 (2006), and under art. 14, Commonwealth v. Moore, 473 Mass. 481, 485 (2016). In Moore, the SJC determined that, "at least with respect to a search of the parolee's home," the reasonable suspicion standard associated with stop and frisk is the appropriate standard for a warrantless search. Id. at 487. Reasonable suspicion for the search of the home was supplied here by an anonymous tip that the parolee was dealing drugs, coupled with evidence of the parolee's conduct consistent with that tip in light of the parole officer's experience with narcotics and with other parolees. Id. at 490.

b) Seizures and Interference with Possessory Interest

Police actions reaching an individual's property constitute a seizure when "there is some meaningful interference with an individual's possessory interests in that property." Commonwealth v. Connolly, 454 Mass. 808, 819 (2009) (internal quotation marks omitted). As Justice Stevens noted in Texas v. Brown, 460 U.S. 730 (1983), "a seizure is usually preceded by a search, but when a container is involved the converse is often true . . . for example, the seizure of a locked suitcase does not necessarily compromise the secrecy of its contents . . . ." Id. at 747–48 (Stevens, J., concurring). Relying on ample precedent from other courts, the Supreme Judicial Court has found the entire computer analogous to such a closed container for seizure purposes. See Commonwealth v. McDermott, 448 Mass. 750, 766 (2007) (agreeing with lower-court "judge's analogy to closed containers with respect to the seizure of the computers and disks"). Whether a seizure has occurred is usually obvious and rarely contested. The following cases concern less-common circumstances.

- Berger v. New York, 388 U.S. 41 (1967). The Court held that wiretaps "seize" conversations in violation of the Fourth Amendment. Id. at 59. The Court did not expand further on how it came to this conclusion, but this case is often cited for the proposition that intangibles (e.g., data) can be seized in the constitutional sense. See, e.g., LeClair v. Hart, 800 F.2d 692, 695 (7th Cir. 1986) ("Following Berger, it has been clear that the Fourth Amendment embraces more than just the forced physical removal of tangible objects . . . . Indeed, Berger stands for the proposition that the government may seize intangible items, such as the information contained in the financial documents which the IRS agents copied.").

- Commonwealth v. Connolly, 454 Mass. 808 (2009). As part of an investigation of a suspected drug dealer, police installed a GPS tracking device in his car. Id. at 10. To install the device, police opened the car's engine compartment, placed the tracking device inside, and attached it to the car's battery. See id. at 812. The Supreme Judicial Court held that installing the GPS device was a seizure within the context of art. 14 of the Massachusetts Declaration of Rights. Id. at 822. First, the installation and presence of the tracker constituted a physical intrusion on the defendant's property. Id. Second, the government's use of the vehicle to obtain information was itself an interference with the defendant's interest in it. Id. at 823 ("It is a seizure not by virtue of the technology employed, but because the police use private property (the vehicle) to obtain information for their own purposes.").

- United States v. Hicks, 438 F. App'x 216 (4th Cir. 2011). Defendant destroyed his hard drive after he found out he was under investigation for possession of child pornography. Id. at 18. After he was convicted of destroying records in a federal investigation, the defendant attacked his conviction on constitutional grounds. Id. One of these challenges was that by criminalizing his destruction of his hard drive, the government had interfered with his possessory interest in that hard drive, effectively seizing it in violation of the Fourth Amendment. Id. at 219. The Fourth Circuit found that there was no meaningful interference with the defendant's possessory interest because he did not have a property right in images of child pornography. Id. (citing Helton v. Hunt, 330 F.3d 242, 247 (4th Cir. 2003), for the proposition that there is no property right in contraband).

The case summarized below discusses the return of unlawfully seized property:

- Commonwealth v. Salmons, 96 Mass. App. Ct. 61 (2019). The defendant pled guilty to assault and battery by means of a dangerous weapon, intimidating a witness, strangulation, and other charges. The police had seized the defendant's three cell phones at the time of arrest, but the seizure was subsequently found unlawful based on the SJC's decision in Commonwealth v. White, 475 Mass. 583 (2016) (probable cause to seize or search a cell phone requires "information establishing the existence of particularized evidence likely to be found there," id. at 593). Salmons, 96 Mass. App. Ct. at 62. The defendant filed a motion for the return of his cell phones, which was granted. Id. at 62. Eight months later, the Commonwealth moved to wipe the content of two of the phones before returning them, because they contained "numerous and sexually explicit photographs and videos of the defendant and [the victim]." Id. The motion to wipe these phones was allowed, id. at 65, but the Appeals Court reversed. Relying on Commonwealth v. Sacco, 401 Mass. 204 (1987), the Court found that "when, as here, property is unlawfully seized without a warrant, cannot be used as evidence, and is not unlawful to possess, it should be returned, upon proper motion, to its undisputed owner or the owner's representative." Salmons, 96 Mass. App. Ct. at 68. There was no factual finding that harm to the victim would occur unless the phones were wiped. Id. at 69. Further, the Commonwealth's reliance on Beldotti v. Commonwealth, 41 Mass. App. Ct. 185 (1997) was misplaced because the public interest standard of G.L. c. 276, § 3 did not apply to property seized unlawfully and because the "connection between the crime and the property here [was] far more attenuated than in [Beldotti]." Id. at 69-70.

c) Private Party Searches

(1) Initial Search Made by Private Party

"[W]hen the state conducts a search in response to information that a private party obtained and communicated to the government, 'the legality of the governmental search must be tested by the scope of the antecedent private search.'" Commonwealth v. Cormier, 28 Mass. L. Rptr. 489, at *4 (Mass. Super. Ct. 2011) (quoting United States v. Jacobsen, 466 U.S. 109, 116 (1984)). Where the government searches something in which a private party has already eroded a suspect's expectation of privacy, the Fourth Amendment is not implicated. Id. (citing Jacobsen, 466 U.S. at 116). Crucially, police examination of

materials "initially discovered and viewed by a private party" can be more thorough than that private party's examination and still fall within the scope of the private party search. Id. at *5 (citing Commonwealth v. Raboin, 24 Mass. L. Rptr. 278, 282–83 (Mass. Super. Ct. 2008)). A more detailed analysis of Commonwealth v. Cormier below demonstrates how the private party search doctrine applies to digital evidence cases.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. at *2. Police found more child pornography at the defendant's house, and he was later charged with possession. Id. The trial judge denied defendant's motion to suppress because the warrantless search conducted by police was within the scope of the preceding private party search. Id. at *4–6. Because the computer technician had previously viewed files from the hard drive, the court found that the defendant's expectation of privacy "had already been eroded," so the subsequent police search did not implicate the Fourth Amendment. Id. at *5.

(2) Warrantless Search: Private Citizen or State Actor

If the intent of a private party conducting a search is not independent of the government's intent, however, the private party becomes an agent of the government, implicating the Fourth Amendment and art. 14. See Commonwealth v. Leone, 386 Mass. 329, 333 (1982). A party becomes a state actor if the police do anything to "solicit, provoke, or tempt" that party into obtaining evidence for them. Commonwealth v. Brandwein, 435 Mass. 623, 631 (2002). The cases below examine the state actor issue in the digital evidence context.

- Commonwealth v. Cormier, 28 Mass. L. Rptr. 489 (Mass. Super. Ct. 2011). Defendant brought a computer hard drive to a data recovery shop. Id. at *1. An employee at the shop copied the files from the damaged hard drive and viewed several of them at random to determine if they had been transferred successfully. Id. Some of the files he viewed contained child pornography. Id. Police then inspected several files from the hard drive to confirm the presence of child pornography before obtaining a search warrant for the drive and the defendant's house. Id. The court found that the data recovery shop employee was not acting as a state agent because he was a private party not acting under the authority of the state. Id. at *4 (citing Commonwealth v. Leone, 386 Mass. 329, 333 (1982), for the proposition that "[e]vidence discovered and seized by private parties is admissible without regard to the methods used, unless State officials have instigated or participated in the search"). The court noted that the employee "made the decision to open the suspicious files . . . as a private citizen, while trying to repair the hard drive at [defendant's] request." Id. The court also found that authorities "did not know that [the defendant] asked [the employee] to repair his hard drive and did not instruct [the employee] to inspect the files." Id. They did nothing "to 'solicit, provoke, or tempt' [the employee] into viewing the files," so he was not a state actor. Id. (quoting Brandwein, 435 Mass. at 631).

- United States v. Lichtenberger, 19 F. Supp. 3d 753 (N.D. Ohio 2014). A private party called police after discovering child pornography on a computer, and the responding officer instructed that individual to boot up the laptop, enter the password, show the images, and gather other devices belonging to the defendant before seeking a warrant. Id. at 754–55. The court found these actions violated the Fourth Amendment because by giving instructions and directing the private party's actions, the police officer made that private party into a government agent. Id. at 758–59. The court therefore suppressed the evidence as having been collected in violation of the Fourth Amendment. Id. at 760.

(3) An ISP's Reporting Obligation Does Not Make it a State Agent

The reporting requirement of 18 U.S.C. §§ 2258A(a) and 2258B(a)—requiring an Internet service provider (ISP) to report any child pornography that it discovers—does not transform an ISP into a government agent when it chooses, voluntarily, to scan files sent on its network for child pornography. United States v. Stevenson, 727 F.3d 826, 829–30 (8th Cir. 2013).

2. Was a Search or Seizure Reasonable?

"The ordinary rule is that to be reasonable under the [Fourth] Amendment a search [or seizure] must be authorized by warrant issued by a magistrate upon a showing of probable cause." Almeida-Sanchez v. United States, 413 U.S. 266, 287 (1973); see also United States v. Carpenter, 138 S. Ct. 2206, 2221 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.") (quoting Riley, 134 S. Ct. at 2482)). This section will lay out the requirements of a valid warrant in the cybercrime context and then highlight some applicable exceptions to the warrant requirement.

a) Warrants

"The Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights require that a warrant be issued only on probable cause, supported by oath or affirmation." Commonwealth v. Nelson, 460 Mass. 564, 568 (2011). Massachusetts law specifically "require[s] an affidavit and an oath." Id. (citing Mass. Gen. Laws ch. 276, §§ 1 and 2B). A neutral magistrate must issue the warrant, see Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971), and it must be particular as to the items to be seized and places to be searched, see Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Warrants must contain information that has not been rendered stale, see United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (to evaluate staleness, courts "must assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information"). In addition, officers must execute warrants in a timely fashion, see Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 329–30 (2014) ("[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event no later than seven days from the date of issuance thereof." (quoting Mass. Gen. Laws c. 276, § 3A)). Warrants must be executed in a reasonable manner. Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). Finally, executing officers must have the signed

warrant with them when commencing the search. The sections below focus on probable cause, particularity, staleness, timely execution, and the manner of executing warrants in the digital evidence context.

(1) Probable Cause / Affidavit

"Under the Fourth Amendment and art. 14, probable cause requires a substantial basis for concluding that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues." Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009) (internal quotation marks and citations omitted) (detailed below). Further:

> The affidavit need not convince the magistrate beyond a reasonable doubt, but must provide a substantial basis for concluding that evidence connected to the crime will be found on the specified premises. Moreover, affidavits for search warrants should be interpreted in a commonsense and realistic fashion and read as a whole, not parsed, severed, and subjected to hypercritical analysis. All reasonable inferences which may be drawn from the information in the affidavit may also be considered as to whether probable cause has been established.

Commonwealth v. Donahue, 430 Mass. 710, 712 (2000) (internal quotation marks and citations omitted).

In order to establish probable cause, law enforcement officials must typically submit an affidavit to a magistrate. That magistrate's probable cause determination is confined to the "four corners" of the affidavit. Commonwealth v. Anthony, 451 Mass. 59, 68 (2008) (detailed below). Probable cause by definition deals with "probabilities," which "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Id. (internal quotation marks and citations omitted). The following cases address probable cause and affidavits in the digital evidence context.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. The warrant affidavit "provided a substantial basis to conclude both that the defendant had committed the homicide [with a] coventurer and that it was reasonable to expect that his cell phone would contain evidence related to that specific crime." Id. at 587. Here, unlike in Commonwealth v. White, 475 Mass. 583 (2016), there was specific evidence of a nexus between the crime and the defendant's cell phone. Id. at 589. This evidence included the following facts: "the defendant made a cell phone call soon after the shooting to the person who rented the car used in the murder, there [was] a reasonable inference that the crime was

preplanned, and there [were] records of threatening cell phone communications between [the defendant's [coventurer] and the victim." Id.

- Commonwealth v. Vasquez, 482 Mass. 850 (2019). The defendant was indicted on charges of murder in the first degree and two related firearms offenses. He moved to suppress witnesses' identification of him from surveillance footage, his statements to the police, as well as evidence obtained from the search of his phone and the CSLI. Id. at 851. The SJC found that the witness identification did not require suppression. But the SJC agreed with the trial court's finding that the Miranda warnings were rendered in Spanish "in such a fragmented and confusing manner so as to be incoherent." Id. at 862. More specifically, the improper translation rendered the warnings "inadequate to apprise the defendant of his rights, and [ ] the defendant's limited comprehension of English did not suffice to compensate for these deficiencies." Id. at 852. Because the Miranda warnings were insufficient and the search of the defendant's cell phone arose from the statements the defendant made after the defective warnings, the search was not sufficiently attenuated from the unwarned statements. Id. at 865. Further, without the tainted information from the unwarned statements (such as the defendant's disclosure of his phone number), the Commonwealth failed to establish "the requisite nexus between the commission of [the] crime and the CSLI for the defendant's device." Id. at 867. The Commonwealth also failed to establish a connection between the crime and the thirty-two days for which it sought CSLI. Id. In sum, the search warrant affidavit did not "support a determination of probable cause, and the CSLI obtained as a result must be suppressed." Id. at 868. The SJC remarked in a footnote, however, that CSLI evidence may be admissible later, if the Commonwealth could show by a preponderance of the evidence that there was an untainted source for the nexus between the crime and CSLI. Id. at 868 n. 27 (quoting Commonwealth v. Estabrook, 472 Mass. 852, 865 (2015)).

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). Following conviction for first-degree murder, the defendant argued on appeal, among other things, that the motion judge erred in denying his pre-trial motion to suppress cell site location information (CSLI) that was introduced as evidence during his trial. Id. at 539. The defendant's brother had identified the defendant as the man leaving the crime scene in video footage, and provided police with a phone number he claimed belonged to the defendant. Id. at 541. Police then requested a court order requiring the service provider to produce CSLI from the cell phone for several months surrounding the day of the crime. Id. at 541. The CSLI placed the owner of the cell phone in the general vicinity of the crime at the time of the killing. Id. The Court ruled that, although it was a close call, the police affidavit in support of a search warrant for historical CSLI satisfied the requirement that "there be a substantial basis to believe that the sought-after CSLI 'will produce evidence of [the] offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed . . . such offense.'" Id. at 545-46 (quoting Commonwealth v. Augustine, 472 Mass. 448, 453 (2015)). The Court rejected the defendant's assertion that the police must demonstrate that the cell phone was used or possessed during the commission of a crime in order to show nexus between "the crime . . . the items sought, and the location to be searched." Id. at 546. This is not necessary because "[c]ell phones physically accompany their users everywhere such that tracking a cell phone results in near perfect surveillance of its user." Id. at 547 (quoting

Commonwealth v. Almonor, 482 Mass. 35, 45 (2019) (internal quotation marks omitted)). The defendant's brother's statement that the cell phone belonged to the defendant, together with subsequent corroboration by the defendant's former girlfriend, was enough to establish the requisite nexus. Id. at 548-49.

- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019). The indictments in this case alleged that the defendant and two co-conspirators broke into the defendant's uncle's home and beat him on the head and face with a crowbar. Id. at 618. The defendant was charged with home invasion, assault, and multiple other offenses. Id. at 618, n. 1. She moved to suppress the fruits of a search of her cell phone. The Superior Court allowed the motion, but the Appeals Court reversed, finding that the police had probable cause to seize the phone, and that the defendant voluntarily consented to an unlimited search of her phone. There was probable cause to seize the cell phone because the defendant told the police it contained videos that "could establish where, when, and with whom the defendant was in the hours before the home invasion." Id. at 623. The police were also aware of multiple facts connecting the defendant to the crime. For example, her car was seen near the victim's home less than two hours before the assault, she had a key to the victim's residence and there was no sign of forced entry, the victim had a restraining order against the defendant, and there were blood stains in the exterior of the defendant's car. Id. In sum, the seizure was lawful because the police had "a substantial basis for concluding" that the phone contained "evidence connected to the crime under investigation." Id. The court also ruled that the defendant's subsequent "consent to search her cell phone was without limitation." Id. at 625-26. The police communicated their intent to search the entire cell phone to the defendant, and she consented to the search, providing the police with passwords to the phone and to her Snapchat account. Id. at 626. Applying "a common sense interpretation" to the defendant's entire exchange with the police detective, the Appeals Court found that her "consent to search her cell phone was free, voluntary, and unlimited." Id.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police approached the defendant sleeping in the stairwell and seized a cell phone on the floor nearby. Id. at 282. There was probable cause to seize the phone because the police "had information that the defendant and victim had been together on the day of the murder, and also that [the murder victim's boyfriend] had recently overheard the defendant confessing to the murder to an unidentified person on a cell phone." Id.

- Commonwealth v. Martinez, 476 Mass. 410 (2017). State police used law enforcement version of P2P client to investigate sharing of child pornography, identified such activity coming from a Massachusetts IP address, and subpoenaed Comcast for information regarding the IP address for the 30-minute period on March 9, 2012, during which police downloaded four suspected child pornography video files shared from the account associated with the IP address. Id. at 411–13. The ISP gave police a name (Angel Martinez) and an address. Id. at 413. Local law enforcement then obtained a warrant to search the apartment located at the address for computers and related items connected to the suspected possession and distribution of child pornography. Id. The apartment was leased to the grandmother of the Comcast account holder and of the defendant (Adalberto Martinez). Id. at 413 n.2. Law enforcement seized two laptops belonging to the

defendant and found five videos containing child pornography on one of them. Id. The SJC held that the affidavit in support of the search warrant (containing information that a particular IP address was used to share child pornography and that this IP address had been assigned at the time to a subscriber at the specific physical address to be searched) was sufficient to establish probable cause for the search, even though the named subscriber was neither listed as, nor confirmed to be, living in the apartment searched, and even though police had no information before the search linking the defendant to the residence. According to the SJC, law enforcement did not have to verify that the account holder lived at the address searched. Id. at 418. Once the nexus between the crime and the service address was established, the names of the account holder and of the leaseholder were incidental. Id. The SJC rejected the argument that law enforcement had to show that the network was secure or that no one outside the address could access the network. Id. at 419. Where the warrant was for the search of a place (not for the arrest of a person), law enforcement needed only demonstrate a sufficient nexus between the criminal activity under investigation, the items sought, and a place to be searched. Id. Even assuming law enforcement could know a network was not secured, unauthorized use of the network did not negate the substantial basis to think the evidence would be located at the address. Id. at 420–21 ("[P]robable cause does not require investigators to 'establish to a certainty that the items to be seized will be found in the specified location,' nor does it require them to 'exclude any and all possibility that the items might be found elsewhere.'" (quoting Anthony, 451 Mass. at 70)).

The decision came with caveats. The SJC cautioned that its decision here does not mean that probable cause always exists any time investigators link illegal computer activity to an IP address and then link that IP address to a physical address. Martinez, 476 Mass. at 422. To support probable cause, law enforcement should use reliable methods—such as the administrative subpoena here—to connect the IP with a physical address, not IP address mapping services. Id. at 423. Additionally, some technologies (e.g., Tor exit relays, VPNs, and proxy server connections, which can mask originating IP addresses) may erode the connection between an IP and a physical address. Id. Law enforcement may be required to disclose in affidavits the possibility that one of these technologies was, or may have been, used based on facts known or reasonably knowable to investigators at the time. Id. "If such technologies become more common, it is entirely possible that we would require police to proceed in multiple steps, obtaining subpoenas related to each intermediary IP address or warrants to search each location hosting those IP addresses." Id. In some cases, law enforcement may be required to determine, by forensic examination of a wireless router, which devices were connected to it and when before searching particular computers. Id.

- Commonwealth v. Perkins, 478 Mass. 97 (2017). "Based on intercepted telephone conversations between defendant's alleged middleman and street-level distributor of cocaine, police surveillance of suspected drug transaction, and other information, the judge issued a warrant authorizing a search of the defendant's apartment for evidence including a cellular telephone and drug-related records." Id. at 99. The warrant also included authorization to seize currency, distribution paraphernalia, documentation about the premises and its contents, among other items. Id. at 101. The affidavit did not seek authorization to search for narcotics. Id. at 98. Police seized a large quantity of cocaine, several cell phones, drug paraphernalia, and ammunition. Id. at 101.

The SJC concluded that the affidavit justified searching the apartment for the defendant's phone. Id. at 105–06. They further concluded that the seizure of nine additional phones found in the apartment was supported by probable cause, but that the police did not have discretion to "search every portion" of these additional phones. Id. At 106. Instead, the plain terms of the warrant restricted their search to call activity and contact lists and did not authorize police to "rummage through the entirety of the defendant's cellular telephones." *Id*. At 106. With regards to searching the defendant's apartment for records, proceeds, and paraphernalia, however, the SJC held that the affidavit:

> did not contain sufficient particularized information to justify [such] a search of the defendant[']s apartment . . . . The affidavit included a single, conclusory statement that probable cause existed based on the affiant's "training and experience and the facts and circumstances learned during the course of this investigation," [but] contained no facts, or opinion based upon the affiant's considerable experience as a narcotics officer, that would have establish[ed] probable cause to believe that the defendant would be likely to store particular items of [drug-related records, proceeds, or paraphernalia] in his home.

Id. at 109.

- Commonwealth v. Jordan, 91 Mass. App. Ct. 743 (2017). In a murder investigation in which defendant was a suspect, police obtained search warrant for his CSLI, call details, text messages, and subscriber information for a six-week period surrounding the date of the homicide. Id. at 744. The Appeals Court found that the trial judge properly suppressed the text messages. Id. Although the affidavit in support of the warrant established probable cause to believe that the victim had been murdered (i.e., a crime had been committed), it made no connection between the defendant's use of his cell phone and his involvement in the crime, and thus did not establish probable cause to conclude that the text messages would provide evidence connected to the crime. Id. at 749–51. The affidavit did establish probable cause to conclude that the defendant committed the crime and showed that the defendant had a cell phone and that it was in use around the time of the murder, and so it established probable cause to believe that the CSLI would provide evidence of the defendant's involvement in the crime. Id. at 750–53. The SJC also held that the trial court had properly suppressed "contact information" insofar as that meant an address book or contact list because the affidavit failed to establish a nexus between the crime and the defendant's contact information. Id. at 753–54. However, if "contact information" meant subscriber information and call records, there was no basis for suppression. Id.

- Commonwealth v. Keown, 478 Mass. 232 (2017). Defendant was suspected of murdering his wife by poisoning her. In the course of the investigation, police obtained a warrant to search his computer and discovered evidence of incriminating Internet searches, which was introduced at trial. Id. at 234–37. The SJC held the affidavit established a sufficient nexus between the crime and the item sought where: (1) it established the defendant's sophistication with computers (he had worked as a Web designer), and showed that he had forged contracts and admissions letter/other communications from Harvard Business School (can infer he used computer); (2) it described forgeries related to the motive alleged in the affidavit, i.e., to kill his wife to prevent her

finding out about their impending financial ruin and his lies and to collect her life insurance benefits; (3) it specified that the victim had died from ethylene glycol poisoning which, the affiant noted, would likely have involved online research. Id. at 238–39.

- Commonwealth v. Broom, 474 Mass. 486 (2016). At the time of defendant's arrest for murder, his cell phone was seized. Id. at 494. Ten months later, law enforcement applied for and obtained a search warrant for its contents. Id. The affidavit contained information about the investigation and the fact that no CSLI information could be obtained for the time surrounding the murder but that the defendant's phone records showed he sent and received text messages and accessed the Internet at the relevant timeframe. Id. It then described the many types of data the detective wanted to search in order to uncover information pertinent to the investigation. Id. at 494–95. The SJC held the search was not supported by probable cause. Id. The Court held that "it is not enough that the object of the search *may* be found in the place subject to search. Rather, the affidavit must demonstrate that there is a reasonable expectation that the items sought *will* be located in the particular data file or other specifically identified electronic location that is to be searched." Id. at 496 (citations omitted) (emphasis in original). Police here already had the defendant's CSLI (except for the time period surrounding the murder) and call records and would have known that the victim's number did not appear in those records. Id. The warrant was also found to be too broad. Id. at 495, 496 n.13.

- Commonwealth v. White, 475 Mass. 583 (2016). A police investigation of an armed robbery and shooting led to the defendant as one of three suspects. Id. at 584. After suspicion focused on him, the detective located his phone, which was held by the defendant's school administrator pursuant to school policy. Id. The detective then "seized the telephone to prevent the defendant from retrieving it and removing evidence or destroying the device." Id. Police had no information at the time indicating that the phone had been used to plan, commit, or cover up the armed robbery they were investigating, or that it contained any evidence of the crime, but instead relied on knowledge that cell phones are frequently used when the offense involves multiple perpetrators. Id. Sixty-eight days after the seizure, police obtained a warrant to search the cell phone and found evidence that was later ordered suppressed. Id. The SJC held that the seizure was not supported by probable cause because probable cause may not be based solely on an officer's opinion that the device is likely to contain evidence of the crime under investigation. Id. at 584–85. "[E]ven where there is probable cause to suspect the defendant of a crime, police may not seize or search his or her cellular telephone to look for evidence unless they have information establishing the existence of particularized evidence likely to be found there." Id. at 590–91. A contrary decision would mean that, where probable cause to charge someone with a crime existed, the person's phone would almost always be subject to seizure and subsequent search. Id. at 591.

- Commonwealth v. Williams, 90 Mass. App. Ct. 1118 (2016) (unpublished). The victim was shot after a drug deal with two suspects. Id. at *1–2. Two witnesses testified that the victim had arranged the deal via phone. Id. Police zeroed in on an 857 (area code) number linked to a person named Patrick Malone. Id. Defendant was then identified as the second suspect and was interviewed by police; he stated that he had known Malone for twenty years and that they had a

phone conversation on the morning of the shooting. Id. at *3–4. Police seized the defendant's iPhone and secured it to get a warrant. Id. The Appeals Court held that "there was probable cause to believe that the defendant's iPhone would contain evidence linking his alleged coventurer Malone to the 857 number and thus to the shooting." Id. at *5. See also Commonwealth v. Perkins, 478 Mass. 97, 105–06 (2017), (where police had detailed and specific knowledge about the defendant's use of a cell phone to arrange drug transactions, and a particular phone number with which that cell phone had been in contact at a specific time, there was probable cause to believe that the defendant used a cell phone to arrange a drug sale and that he had done so on other occasions and the seizure of nine cell phones from his apartment was proper). But see Commonwealth v. Fulgiam, 477 Mass. 20, 34 (2017) (where warrant application established a personal relationship between defendant and victim and the circumstances of the murders suggested a connection to drugs, it did not, without more, justify intrusion into the content of the communications between defendant and victim).

- Commonwealth v. Finglas, 81 Mass. App. Ct. 1102 (2011) (unpublished). Police were sent information about the defendant, whose email address had received five images depicting child pornography. Id. at *1–2. On interlocutory appeal, the Appeals Court granted the defendant's motion to suppress evidence obtained as a result of a search of his residence. Id. at *3. It did so because the affidavit in support of the warrant was "inadequate to establish a timely nexus between the defendant and the location to be searched and to permit the determination that the particular items of criminal activity sought reasonably could be expected to be found there." Id. The Appeals Court held that the affidavit did not provide any evidence that a computer at the residence had been used to search for or download any child pornography or that the defendant had actually accessed the emailed images. Id. at *2. Further, a police officer's opinion about the common practices of child pornography collectors was not enough, without further facts, to support a finding that the defendant's computer likely contained child pornography. Id. at 3.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it based on an affidavit alleging: (1) both shared folders had a copy of the same pirated movie, (2) the second computer's shared folder had child pornography, and (3) the defendant stated he could not guarantee there was no child pornography on his computer. Id. at 105, 107–09. The Court invalidated the search warrant because it found police did not provide a "substantial basis" to believe there would be child pornography on the computer. Id. at 111. The Court found it unreasonable to infer that somebody interested in sharing a commercial movie would also be interested in sharing child pornography. Id. at 112. That the defendant had access to child pornography did not help the Commonwealth's case. Id. Nor was a suspicious statement, standing alone, enough to provide the substantial basis necessary for probable cause. Id. at 113.

- Commonwealth v. Anthony, 451 Mass. 59 (2008). Police received a tip about a person soliciting child pornography online. Id. at 60–62. They traced these solicitations to a library and arrested a

homeless suspect there. Id. at 62–63. Shortly after the arrest, the suspect took a receipt (along with other pieces of paper) out of his pocket and tore it up. Id. at 63. This receipt was from a repair shop for the repair of two laptops. Id. Police also determined he rented a storage locker. Id. at 64. Police sought and received a search warrant for the locker, the laptops, and a hard drive from the library. Id. at 65–66. A superior court judge granted the defendant's motion to suppress for lack of probable cause, however, and the Commonwealth pursued an interlocutory appeal. Id. at 67–68. The SJC reversed the motion judge's suppression of the warrant, finding the affidavit established probable cause. Id. at 73. Specifically, the Court found information about the suspect's prior conviction for child pornography, the outside tip, and the suspect's admission to viewing child pornography in violation of his probation established probable cause for the crime. Id. at 70–71. From there, it found the fact that a homeless individual rented a storage locker using a false address—along with the detective's experience that viewers of child pornography tend to collect it—supported the idea that the suspect might hide child pornography at his storage locker, the only space under his control. Id. at 71–72. The Court found the suspect tearing up the receipt supported the inference that he was trying to hide child pornography. Id. at 71. It emphasized that the affidavit did not rely solely on the opinions of the affiant with respect to general characteristics of collectors of child pornography. Id. at 72. Rather, the affidavit contained enough facts and inferences to support a nexus between the alleged crime and the locations to be searched. Id. 72–73.

(2) Independent Source Doctrine

- Commonwealth v. Wilson, 486 Mass. 328 (2020). The police initially obtained defendant's CSLI data pursuant to an § 2703 order, without a warrant, in 2010. Id. at 336. The CSLI placed the defendant in "the victim's hotel, at the commuter lot where the [victim's] rental vehicle was found, and in the location where the victim's body would later be discovered, at relevant times on the night of the murder." Id. at 331. In 2014, the police obtained the same CSLI information pursuant to a search warrant. The Court found that the 2014 warrant satisfied the "independent source doctrine," "a well-recognized exception to the exclusionary rule under both the Fourth Amendment and art. 14." Id. at 335. The doctrine provides that "evidence initially discovered as a consequence of an unlawful search may be admissible if later acquired independently by lawful means untainted by the initial illegality." Id. (quoting Commonwealth v. DeJesus, 439 Mass. 616, 624 (2003)). Here, the affidavit supporting the 2014 warrant for the CSLI was based on facts wholly independent of the CSLI data obtained in 2010. Id. at 336. These facts included the following: the defendant's public statements about having a firearm like the one used in the murder, his status as the likely father of the victim's unborn child, causing financial obligations to the victim and the "ire of the defendant's wife," the victim's statement to a friend that the defendant asked her to get an abortion, the cellphone communications between the defendant and the victim until shortly before the victim's cellphone activity ceased at 10:49 P.M. on the night of the murder, and a Facebook message from the victim's account after she was reported missing "claiming she was in the hospital after an abortion, although police determined that she was not a patient at any area hospitals." Id. at 337.

- Commonwealth v. Gosselin, 486 Mass. 256 (2020). The defendant appealed his conviction for first-degree murder, arguing, *inter alia*, that his trial counsel was ineffective for not moving to

suppress CSLI evidence, as such evidence provided probable cause for the search warrant for his home—the search of which produced critical inculpatory evidence. Id. at 264. The Court declined to resolve whether the § 2703 warrant was supported by probable cause, on the grounds that "the search warrant affidavit satisfied probable cause when excising the unconstitutionally obtained CSLI," such that the defendant failed to demonstrate prejudice and his trial counsel was not ineffective. Id. at 264-66 & n.9.

(3) Particularity / Scope

The Fourth Amendment, art. 14, and Mass. Gen. Laws ch. 276, § 2 all require that search warrant applications particularly describe the places to be searched and the items to be seized. See Commonwealth v. Valerio, 449 Mass. 562, 566 (2007). Massachusetts courts treat these provisions as coextensive. Id. The dual purpose of these requirements is (1) to protect people from general searches and (2) to provide the Commonwealth the opportunity to demonstrate to a court that officers' search authorization was properly limited. Id. Additionally, the requirement provides essential information to a person whose property is being searched. Id. (citing Katz v. United States, 389 U.S. 347, 356 (1967)). The cases below explore the tension between the particularity requirement and the amorphous nature of data in the digital era.

- Commonwealth v. Snow, 486 Mass. 582 (2021). The defendant and two other men were arrested in connection with a fatal shooting that occurred earlier on the night of the arrest. Id. at 583. Prior to trial, the defendant successfully moved to suppress evidence found on his cell phone. Id. He argued that there was no probable cause for the cell phone search warrant because the warrant affidavit failed to establish a sufficient nexus between the murder and the defendant's cell phone. Id. The Commonwealth appealed, and the SJC reversed, finding that there was probable cause for the search. Id. However, the Court concluded "that the search of the phone was not sufficiently particular because it lacked any temporal limit." Id. at 583. More specifically, the Court held "that (1) the correct remedy for the warrant lacking particularity in this case [was] partial suppression; (2) the search of text messages, call logs, and Snapchat video recordings was proper; yet (3) the lack of time restriction rendered the warrant impermissibly broad." Id. at 590. Accordingly, the SJC remanded the case to the Superior Court to determine whether "the proffered evidence fell outside what would have been a reasonable temporal limit." Id. First, as to partial suppression, the Court noted "that an overbroad warrant generally requires only partial suppression of the information for which there was not the requisite nexus, as long as the Commonwealth had not relied on or otherwise exploited it at trial. Id. at 591-92 (quotations and citations omitted). Second, because the police here had probable cause to search the defendant's cell phone for evidence of joint venture, the scope of the search properly included communications such as call logs, text messages, and Snapchat videos. Id. at 593. Third, a cell phone search warrant cannot be sufficiently particular without some temporal restriction that should "err on the side of narrowness." Id. at 594. Where the initial search provides probable cause to broaden the search, "nothing precludes" officers from requesting another, broader warrant. Id.

- Commonwealth v. Wilkerson, 486 Mass. 159 (2020). In a more recent case involving partial suppression of CSLI, the government requested 48 hours of a shooting suspect's CSLI around the time of the shooting, received 34 hours of CSLI in response to this request, and then had all but

three hours of CSLI ("covering the period approximately ninety minutes before and ninety minutes after the shooting") suppressed by the trial judge. Id. at 164. The SJC upheld this partial suppression of CSLI data, but noted in dicta that the "severance doctrine [of Hobbs] is not without limits," and that "where a warrant so lacks particularity or is so overbroad that it begins to resemble a general warrant, total suppression is required." Id. at 168-69. The court deemed the CSLI request at issue "not so overbroad on the facts of this case so as to be akin to a general warrant" and found it to "represent 'a reasonable period of time encompassing the commission of and flight from the crime.'" Id. at 169 (quoting Hobbs, 482 Mass. at 550). However, the SJC declined to provide further guidance on exactly "how overbroad a request for CSLI must be in order for total suppression to be appropriate." Id.

- Commonwealth v. Hobbs, 482 Mass. 538 (2019). The government requested three and a half months of historical CSLI from defendant's cell service provider, from December 1, 2010 to March 15, 2011, where defendant was a suspect in a December 16, 2010 killing. Id. at 543, 550. "This extended request was in part the result of the failure to identify the defendant as a suspect for nearly two and one-half months, and the absence of any evidence of his current location once he was identified as a suspect." Id. at 550. The SJC considered the question of whether "either the Fourth Amendment or art. 14 require[s] total suppression of the entire amount of CSLI collected," or whether "the proper remedy [is] to suppress only the CSLI for which there is not the requisite nexus to the crime," and concluded that "where the requisite nexus for probable cause clearly exists for a reasonable period of time" contained within the requested period, "the CSLI for [the relevant] period of time need not be suppressed so long as the CSLI for which there is not the requisite nexus to the crime is not relied on or otherwise exploited by the Commonwealth at trial." Id. However, the court suggested its holding was fairly narrow, noting that "[g]iven the uncertainty in the case law regarding overbroad requests for CSLI, we proceed cautiously on this issue." Id. The Court also "emphasized the significant constitutional issues raised by the collection of extended amounts of historical CSLI, and the importance of limiting the requests accordingly." Id. at 550 n.13.

- Commonwealth v. Holley, 478 Mass. 508 (2017). In a murder investigation, law enforcement examined the victim's call records and learned that the last call the victim answered before the shooting came from the defendant's telephone number. Id. at 511. Law enforcement then obtained cell phone records through a warrant served on the carrier and found multiple incriminating communications via text and call between the victim and the defendant's joint venturer. Id. The warrant for the phone records sought "subscriber information; billing records and detailed airtime; outbound call detail; call origination and termination location; stored GPS location information, and/or stored cellular tower records, cell tower sector information, range from cell tower information (RTT) and physical address of cell sites; and all stored contents of electronic or wire communications including stored or deleted voicemail, read, unread, deleted, or sent electronic mail or text messages, and stored files; and listing of all associated phone numbers, of a subscriber to or customer of such service" between October 1 and 18, 2012. Id. at 524–25. The broad scope of the search raised "significant concerns" for the SJC because it did not sufficiently limit the scope of the search so as to prevent "exploratory rummaging." Id. at 525,

528. But because the record was silent on how the provider conducted the search and on what information, if any, it provided to the Commonwealth beyond the text messages (it was even unclear whether the provider kept any stored content apart from text messages as part of its business records) and because the only communications used at trial were the defendants' redacted text messages from four and two days before the shooting, respectively, the day of the shooting, and the day after the shooting, the Court could find no error in the denial of the motions to suppress. Id. at 525 (noting that the "Commonwealth did not capitalize on the lack of particularity in the warrant").

- Commonwealth v. Molina, 476 Mass. 388 (2017). Police investigating a P2P network found child pornography shared by a Massachusetts IP address. They subpoenaed Verizon and obtained a name (Hermes Delcid) and service address. Id. at 390–91. Further investigation found the name on the mailbox outside of the address and RMV records showed Delcid at the address. Id. at 391. Police then obtained a search warrant for the apartment and in particular for electronic devices containing evidence of child pornography, evidence of child pornography in other formats, evidence related to access to the Verizon account and the P2P network, and evidence related to access to electronic devices at the apartment. Id. In a bedroom later identified as the defendant's, police observed the P2P program running on an open laptop (computer screen showed downloads and uploads of child pornography files in progress). Id. at 392. The search team seized numerous electronic devices from the apartment, including the defendant's laptop and desktop computers and his external hard drive. Id. On appeal, the defendant argued that the search warrant was impermissibly overbroad as to both places and "things" to be searched. Id. at 393. The SJC disagreed. Id. at 389. It found that the warrant appropriately substantiated a connection between the apartment and the evidence of child pornography reasonably expected to be located therein. Id. at 394. That the apartment was shared by multiple people was immaterial because the warrant authorized a search of the location associated with the IP address, not a search of any single associated subscriber. Id. at 395. Computer devices using the monitored IP could have been anywhere in the apartment, so where the defendant's unlocked bedroom showed no indicia of separate ownership from the rest of the apartment, the search of his bedroom was proper. Id. at 396. With regard to the things to be searched, the SJC made the following finding: "Because that evidence, in the form of electronic files, could be easily transferred between devices at the same location, police need not have limited the devices to be searched. Id. at 396. The SJC raised the reasonableness of the search *sua sponte*. Id. at 397. It found that where "multiple electronic devices that may well belong to multiple individuals are seized and searched, the reasonableness of the undertaking will be judged, at least in part, by whether the searches of those devices are conducted in a manner that seeks to limit the scope of the search as much as practicable in the particular circumstances." Id. at 397–98. The SJC may in the future "consider whether to require, as some courts have, a digital search protocol that would affirmatively demonstrate 'a high regard for rights of privacy and take all measures reasonable to avoid unnecessary intrusion.'" Id. at 398 (quoting Commonwealth v. Vitello, 367 Mass. 224, 262 (1975)).

- Commonwealth v. Keown, 478 Mass. 232 (2017). "The scope of the search authorized by the warrant included files on the laptop related to the health or death of the victim; other prominent

poisoning cases; ethylene glycol or other poisons; and the financial records, life insurance plans, and wills of the victim and the defendant." Id. at 240. The affidavit "established probable cause to search for evidence on the laptop computer relating to the defendant's role in his wife's death." Id. "These categories of evidence were related to the means of committing the crime and the motive of the defendant, and provided sufficient guidance to the examiners so that they were not on a fishing expedition." Id. In addition, the search was conducted reasonably. Id. at 241. Examiners used a list of 50 search terms that was later supplemented by 19 additional terms. While not part of the warrant application, the terms were related to the categories of evidence sought in the affidavit. "[T]he examiner only looked closely at approximately 325 files of the nearly 400,000 found on the laptop computer." Id. The search in this case "took place more than a decade ago in an entirely different technological landscape"; thus, the absence of an ex ante search protocol did not defeat particularity. Id. at 41.

- Commonwealth v. Dorelas, 473 Mass. 496 (2016). The defendant, who was a suspect in an assault and battery by means of a dangerous weapon (firearm) and an assault with intent to murder, was involved in a shooting. Id. at 497. Interviews with his family and friends indicated that prior to the shooting he had received threatening calls and texts. Id. at 498. Police believed the defendant's iPhone contained evidence linking the defendant and the other shooter to the assaults and obtained a warrant authorizing a search for, among other things, saved and deleted photographs. Id. at 498–99. The search resulted in the discovery and seizure of incriminating photographs. Id. at 499. The defendant contended that police only had probable cause for his call logs and text messages, but not his photographs. Id. at 500. On direct appellate review, the SJC reached the following holding: "Communications can come in many forms including photographic, which the defendant freely admits. So long as such evidence may reasonably be found in the file containing the defendant's photographs, that file may be searched." Id. at 503. Therefore, such a search is "neither outside the scope of the warrant nor unreasonable." Id. The defendant further argued that a search using the Universal Forensic Extraction Device (UFED) could have been conducted for communications, including photographic communications, without reviewing his photograph file. Id. at 504. The SJC held that such a retrieval method was not constitutionally required where the photographic evidence would also reasonably be found in the phone's photograph file. Id. The Court was concerned that texts and their attachments might be overwritten over time and the evidence would thus only be found in the photograph file. Id.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the shooting. Id. at 764–65. They seized five computers and disks. Id. at 765. The defendant asserted that this was unlawful because the warrant did not specifically authorize the seizure of these items. Id. at 770. The warrant did authorize, however, seizure of several types of documents. Id. at 771. The Court held that the seizure of the computers was reasonable because they functioned as "closed containers" storing documents. Id. at 766, 771. [Note: In Preventative Medicine Assocs. v. Commonwealth, 465 Mass. 810 (2013), the SJC clarified that in McDermott, the fact that the warrant was issued before an indictment as part of an investigation and the Commonwealth's use of preset search terms during the preliminary review of the defendant's

files were important to its holding, id. at 830–32. The Court stated that it took "seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained." Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.]

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. 2001). Police received information that defendant was distributing child pornography over the Internet. Id. at *1. They obtained a warrant allowing them to seize the defendant's computers and associated storage devices, to bring those items to a search location, and to search them for "visual images depicting children in a state of nudity or sexual conduct." Id. at *8. The defendant challenged the warrant as not particular enough because it allowed for seizure and search of all files on the computer, many of which were not related to child pornography. Id. The court denied the defendant's motion, noting that "where the commingling of legitimate and illegitimate items makes an on-site examination impracticable, a temporary seizure of the whole is permitted." Id. (citing various federal cases to that effect). It noted that "[t]he investigators could not have known in what form—whether on the computer hard drive or other various storage devices—the defendant was storing the target images. To insulate such images from search and seizure merely because other, non-incriminating items may have sheltered the images would pervert the accepted purpose of the constitutional bar against general searches." Id. at *9.

- United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013). Police received a tip that a Washington resident was sharing child pornography over a peer-to-peer networking site. Id. at 1043. They prepared a search warrant affidavit setting forth the information they had received about the suspect's IP address, the pornography he shared, general peer-to-peer network operations, data storage, and known characteristics of child pornography offenders. See id. The magistrate granted the warrant, which authorized seizure of all of the defendant's computers and data storage devices, and police discovered large quantities of child pornography. Id. at 1043–44. The trial judge suppressed the evidence reasoning that the warrant was facially overbroad. Id. at 1045. The Ninth Circuit reversed this decision. Id. at 1046. It based this ruling on the "practical, common-sense decision" judges make in issuing warrants. Id. at 1046. Specifically, the Ninth Circuit found that "[t]he government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files" and reasoned that "[t]he government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner." Id. Given this reasoning and supportive precedent, the court found the warrant permissible. Id. at 1047.

- In re a Warrant for All Content & Other Info. Associated with Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386

(S.D.N.Y. 2014). Federal agents investigating illegal money remitting applied for a search warrant to access a suspect's entire email account in search of specified emails. Id. at 388. The Magistrate considered and rejected the reasoning that such a search was akin to a general warrant and therefore failed the Fourth Amendment's particularity requirement. Id. at 390–91. First, the judge noted that extensive authority supported the proposition that investigators could briefly examine a wide variety of documents during a search in order to determine relevance. Id. at 391–92. Though that examination is essentially a seizure, it is also a practical necessity to determine which documents can be more permanently seized. Id. at 392–93. Next, he noted that courts have been more flexible with searches and seizures of electronic evidence because the large mass of undifferentiated information makes an on-site search impossible. Id. at 392. Courts have recognized the practical necessity of copying hard drives for later examination, allowing the government to access electronic information outside the scope of its search in order to effectuate that search. Id. at 393. Finally, the judge found that email provider employees would not be capable of performing the search themselves because they would not know enough about the investigation in order to properly recognize relevant emails. Id. at 395.

(4) Staleness of Information Supporting Probable Cause

In order to provide probable cause sufficient for a search warrant, the information contained in an affidavit supporting such a warrant must be sufficiently fresh. See United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (detailed below). In assessing staleness, courts "do not measure the timeliness of information simply by counting the number of days that have elapsed" but rather "assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." Id. (citing United States v. Pierre, 484 F.3d 75, 83 (1st Cir. 2007)). This requirement should not be confused with the separate Massachusetts statutory requirement (examined next) that warrants be timely executed after they have been issued. The following cases address staleness in the digital evidence context.

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that affidavit in support of the warrant to search his home did not establish probable cause because it was based on stale information: namely, an image depicting child pornography that was uploaded from the defendant's computer to the Skype service seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time (id. at 29), the Court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the Court identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a

single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]" – an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020). Defendant was convicted of unlicensed carrying of a firearm outside his residence or place of business. Id. at 420–21.The police obtained a search warrant based an affidavit that described (1) a series of images and videos of the defendant and an acquaintance handling a TEC-9 firearm at the acquaintance's house, which the two of them posted on Snapchat, and (2) location data from a GPS device that the acquaintance, Santos, who was subject to GPS monitoring, was wearing at the time of the Snapchat posts. Id. The defendant argued that because "Snapchat videos and images that are posted on a particular date may have been taken, created, or recorded at an earlier date and uploaded much later… the Commonwealth failed to prove that the information officers relied on from the timestamps on the defendant's and Santos's Snapchat uploads was not stale." Id. at 424. The court rejected the defendant's arguments on staleness, finding probable cause was established by a Snapchat post by Santos from two days before the search warrant was obtained and executed: an image of a TEC-9 (semiautomatic) firearm captioned "Shyt change on my block trust issues I got put all my trust in semi autos." Id. at 421, 424. The court characterized the caption as "a present tense statement about Santos's perceived need for semiautomatic weaponry[, g]iven [which] there was probable cause to believe that the Snapchat image was taken contemporaneously with its posting" (which, in turn, was only two days before the warrant was executed). Id. at 424. The court did not discuss whether, or under what circumstances, similar posts absent such a present-tense caption could have sufficed to establish probable cause.

- Commonwealth v. Cruzado, 480 Mass. 275 (2018). Police waited ten days to apply for a search warrant on a seized phone. See id. at 283. This delay was permissible because "the defendant's minimal possessory interest was far outweighed by the government's interest in obtaining evidence regarding a recent murder." Id.

- United States v. Morales-Aldahondo, 524 F.3d 115 (1st Cir. 2008). Defendant was convicted of possessing child pornography as a result of an investigation targeting a child pornography website and its subscribers. Id. at 117–18. The download information obtained from the website was over three years old by the time the search warrant in this case was issued. Id. at 119. On appeal, the court upheld the trial judge's denial of the defendant's motion to suppress for staleness. Id. Focusing on the characteristics of child pornography collections, the court found that the warrant application (along with testimony by the same officer during a subsequent Franks hearing) "provided considerable support for the government's position that customers of child

pornography sites do not quickly dispose of" their collection. Id. Given this support, the court found that three years was not so long a period that the information had become stale. Id.

- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished). In this case, the Attorney General's Office investigated the defendant based on a tip they had received from a New Hampshire police officer. Id. at *1. Using information from online exchanges the defendant had with the officer four months prior, the AG's Office obtained a search warrant for the defendant's premises where they located the evidence at issue in this case. Id. at *1, *6. The defendant alleged that the warrant was defective because, among other reasons, "there was no temporal proximity between the events constituting probable cause and the issuance of the warrant." Id. at *5. The court rejected this argument for two reasons. First, it found that the affidavit demonstrated continuous contact between the defendant and the undercover officer for several months. Id. at *6. Even though that information was itself four months old, the court found that it gave rise to an inference that the contact had continued. Id. Second, the court focused on the special circumstance of transmitting child pornography via computer. Id. at *7. Specifically, the affidavit described how computers retain data and how collectors of child pornography tended to retain those collections for long periods. Id. The court found that these descriptions "provided the magistrate with reason to conclude that the passage of time did not constitute a disabling tardiness." Id.

(5) Timely Execution of the Warrant

Mass. Gen. Laws ch. 276, § 3A, provides that "[e]very officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event not later than seven days from the date of issuance thereof . . . ." Mass. Gen. Laws ch. 276, § 3A (2018); see also Fed. R. Crim. P. 41(e)(2)(A) (requiring return of a warrant within fourteen days in federal courts). Given the complexities inherent in searching digital devices, the requirement that warrants be executed within seven days of issue could prove burdensome when investigating computer crimes. Fortunately, Massachusetts courts have interpreted the provision liberally with regard to digital evidence, as the cases below demonstrate.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. Relying on the reasoning in Commonwealth v. Kaupp, 453 Mass. 102 (2009), the court concluded that "if police have obtained a warrant to search and seize evidence from a cell phone in their custody, they must *attempt* but need not *complete* a forensic examination of the device within seven days of the warrant's issuance," id. at 330 (emphasis added) (Commonwealth v. Kaupp is summarized below). The court provided no guidance about what exactly constituted an "attempt" to conduct a forensic examination.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's computers. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized the first computer and then received a search warrant for it. Id. at 105–06. Though the Supreme Judicial Court invalidated the warrant on probable cause grounds, it noted that, had the warrant been valid, the fact that it took more than seven days to fully search the computer would not have required suppression. Id. at 114–15. The Court cited other jurisdictions in support of the proposition "that the police do not need to complete forensic analysis of a seized computer and other electronic data storage devices within the prescribed period for executing a search warrant." Id. at 115. The Court held that a written return listing the devices to be examined that was filed within seven days after the search warrant issued satisfied Mass. Gen. Laws ch. 276, § 3A. Id.

(6) Manner of Executing the Warrant

"Under both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, the manner in which a search is conducted must be reasonable." Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 822 (2013). The cases below deal with this requirement in the digital evidence context.

- Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810 (2013). This case dealt with the search of a defendant's email account after indictment, and the possibility of intercepting privileged communications. Id. at 811. The Court held that "[w]hen an indicted defendant's e-mails are the object to be searched by the Commonwealth, because there is a risk that they contain privileged communications . . . a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege." Id. The SJC distinguished McDermott in part on the ground that the warrant in that case was issued before an indictment as part of an investigation, and the Commonwealth used preset search terms during the preliminary review of the defendant's files. Id. at 831. The Court stated that it took

  > seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14, particularly where—as the Commonwealth appears to argue would be permissible and appropriate in this case—the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained.

  Id. at 831–32. The SJC did not rule on these issues in Preventative Medicine, however, because a search had not yet been conducted in that case. Id. at 832.

- Commonwealth v. McDermott, 448 Mass. 750 (2007). After a deadly mass shooting, police officers searched the defendant's apartment pursuant to a warrant for evidence linking him to the

shooting. Id. at 751, 764–65. As part of that search, they seized computers and disks. Id. at 765. The Court upheld this seizure as reasonable because it recognized the impracticality of searching computers on-site. Id. at 776. It also analogized this seizure to that of a firearm, stating that it "must be listed in the inventory taken from the premises in the timely return of the warrant but it may be submitted for specialized examination at an off-site forensic setting for the further extraction of evidence." Id. (citation omitted). The Court stressed the need to minimize the intrusion caused by digital searches. Id. at 777. In this case, police met that burden through the procedure they employed: "A forensic duplicate was made of the . . . hard drives and storage media to preserve all original data," and investigators used a keyword search that "resulted in a cursory inspection of only approximately 750 files . . . which amounted to less than one per cent of the defendant's files." Id. The Court also suggested that "[i]n conducting the actual search . . . considerable discretion must be afforded to the executing officers regarding how best to proceed" and that "[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary." Id. at 776.

b) Exceptions to the Warrant Requirement

"Warrantless searches are per se unreasonable unless they fall within one of the few narrowly-drawn exceptions to the warrant requirement." Commonwealth v. Durham, No. 9610398, 1998 WL 34064623, at *2 (Mass. Super. Ct. Oct. 13, 1998). "When a warrantless search is conducted, the Commonwealth has the burden of showing that the search, and any resulting seizure, falls within this narrow class of permissive exceptions." Id. The sections below examine searches incident to arrest, the plain view doctrine, and exigent circumstances in the digital evidence context.

(1) Search Incident to Arrest

One of the recognized exceptions to the warrant requirement is for searches made incident to a suspect's arrest. In Massachusetts, such searches are governed not only by the Fourth Amendment and art. 14 but also by Mass. Gen. Laws ch. 276, § 1, which is generally seen as more restrictive than the Fourth Amendment. See Commonwealth v. Blevines, 438 Mass. 604, 607 (2003). This statute permits searches incident to arrest "only (1) for the purpose of seizing evidence of the crime for which the arrest has been made in order to prevent its destruction or concealment or (2) for the purpose of removing any weapon the person arrested might use to resist arrest or to escape." Id. (quoting Commonwealth v. Wilson, 389 Mass. 115, 118 (1983) (internal quotation marks omitted)).

Whether the search is permissible is based on an objective standard, so an officer's subjective intent as to the search is irrelevant as long as the search could reasonably have been expected to uncover weapons or evidence facing destruction. Id. at 608 (permitting removal of defendant's car keys from his pocket during search because an officer "discovering a hard object in [a] defendant's rear pocket, [is] justified in retrieving that object as a potential weapon"). Further, having removed an item, "police need not ignore obvious aspects of or markings on" it, id. at 609 (citing Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 770 (1989)), but "detailed scrutiny" is disallowed, id. The cases below involve digital evidence in the context of a search incident to arrest.

- Riley v. California, 134 S. Ct. 2473 (2014). In two consolidated cases, law enforcement officials inspected the contents of an arrestee's cell phone—citing the search incident to arrest (SITA) exception—and used information therefrom in aid of further investigation. Id. at 2480–82. The Supreme Court held that these searches did not fall within the SITA exception because the justifications undergirding the exception did not apply to cell phones. Id. at 2484–85. First, digital contents of a cell phone cannot pose an immediate risk of physical injury to an officer. Id. at 2485–86. Second, once the phone has been seized by law enforcement (which the Court did allow), the arrestee cannot hide or destroy any evidence thereon (at least according to the Court). Id. at 2486. Confronting the issues of automatic locking, encryption, and remote wiping, the Court expressed doubt that these issues were particularly common, drew a distinction between such actions and the arrestee-initiated destruction of evidence in a typical SITA exception case, and allowed police to employ other means of preventing such actions. Id. at 2486–88 (noting that police may power off the phone or block its network connection and hypothesizing that the police may be allowed to alter a phone's settings to prevent it from locking). Finally, the Court noted that in exceptional cases—such as an imminent threat that the phone will be remotely wiped—the exigent circumstances exception may apply on a case-by-case basis. Id. at 2487–88.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone, James provided it, and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The

image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC held that the warrantless search of the digital camera was not a valid search incident to arrest under art. 14 of the state constitution. Id. at 592–93; see also id. (declining to address the constitutionality of the search under the Fourth Amendment). The SJC applied Chimel and Riley and found the twin threats of "harm to officers and destruction of evidence" were not present with regard to the data on a digital camera. Id. at 592. The SJC reasoned that, once the camera was secured, the data on it posed no danger and the risk of destruction of evidence was mitigated (and was less of a concern with respect to digital cameras lacking network connectivity than with cell phones). Id. at 592–93.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Police apprehended the defendant after giving chase to two men. Id. at 550. Defendant claimed he was not one of the two men. Id. When asked why he was breathing heavily, he claimed to have been arguing on the phone with his girlfriend. Id. at 550–51. After he was booked, the defendant placed a phone call he claimed was to his girlfriend. Id. at 551. Police then examined his cell phone call log about five hours after the arrest, without obtaining a warrant; the log belied both of defendant's statements. Id. The booking sergeant testified that it could take several days to get a warrant, and that he was concerned that incoming calls would "push out" previous calls on the call log, which he believed permitted only a limited number of calls. Id. The SJC held that under Riley (described above), decided a year earlier, the search of the call log was not a proper search incident to arrest and was not justified by exigent circumstances. Id. at 557. The SJC found that—absent testimony suggesting the phone was password protected or that police were concerned about remote wiping—preservation of the call log could have been achieved by "turning the cell phone off, placing the cell phone in a Faraday bag, or securing the cell phone and seeking a warrant for it." Id. at 558–59.

(2) The Plain View Doctrine

Under the plain view doctrine, law enforcement may make a warrantless seizure of evidence when four conditions are met. See Commonwealth v. Ericson, 85 Mass. App. Ct. 326, 333 (2014) (explained below). First, the officers must lawfully be in a position to view the evidence. Id. Second, they must have a lawful right of access to the object. Id. Third, they must have a reason for seizing it. Id. In cases concerning (a) items possessed illegally, the incriminating character of the object should be immediately apparent. Id. (citing Horton v. California, 496 U.S. 128, 136 (1990) (explained below)). In cases concerning (b) other types of evidence, the particular evidence must plausibly be related to criminal activity of which the police are already aware. Id. (citing Commonwealth v. Sliech-Brodeur, 457 Mass. 300, 306–307 (2010)). Fourth, art. 14 requires that police come across the object inadvertently. Id. (citing Sliech-Brodeur, 457 Mass. at 307). The following cases address the plain view doctrine in the digital evidence context.

- Commonwealth v. Tarjick, 87 Mass. App. Ct. 374 (2015). Defendant's stepdaughter disclosed he abused her and took sexually explicit photos/made recordings of her. Id. at 375. Police obtained a warrant authorizing the search of the defendant's home and the seizure of the defendant's cell phone, the family computer, and the family video camera. Id. Three memory cards that were in the camcorders or digital cameras were also seized when the warrant was executed, though they

were not included in the warrant. Id. A second warrant was obtained to search the contents of the memory cards and evidence from the cards was later used at trial. Id. at 375–76. The Appeals Court held that the seizure was within the plain view exception. Id. at 378. The cards, though not included in the original warrant, were plausibly related to the crime. Id. "The officers were . . . aware that data may be freely transferred from one device to another through memory cards, and they could reasonably have concluded that the memory cards might have contained the alleged recordings." Id. The inadvertence requirement was also satisfied because there was "no indication that the police had probable cause to believe, prior to the search, that these specific memory cards or the cameras containing them would be found." Id.

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014). Defendant in this case texted with a young girl—and subsequently with the police officers to whom she gave her phone—asking for nude photos. Id. at 327–28. As part of this exchange, the defendant sent a photo of himself in a tank top from the waist up. Id. at 328. Upon obtaining the phone, police received a warrant to search for, among other things, the tank top image. Id. at 329. While examining the phone, they discovered three images of the defendant's penis, which served as the basis of his conviction for possession of matter harmful to minors with intent to disseminate. Id. at 329, 334. On appeal, the court upheld this seizure under the plain view doctrine. Id. at 333. Fulfilling the first and second plain view requirements, the warrant authorizing seizure of the tank top image means the police "were lawfully situated to view and to secure the [penis] images" because police are authorized to conduct cursory inspection of computer files to determine whether they match items listed in the warrant. Id. at 333–34 (citing Commonwealth v. McDermott, 448 Mass. 750, 776–77 (2007)). Third, the images of the defendant's penis were plausibly related to criminal activity of which the police were aware. Id. at 334. The defendant's statements of intent to exchange pictures of his nude body with pictures of the minor gave police reasonable ground to believe the pictures were evidence of enticing the minor to pose in a state of nudity. Id. The same statements made it plausible that the pictures were evidence of possession of matter harmful to minors with intent to disseminate. Id. Fourth, police discovered the images inadvertently because they "lacked probable cause to believe, prior to the search, that specific items would be discovered during the search." Id. (quoting Commonwealth v. Balicki, 436 Mass. 1, 9–10 (2002)).

- United States v. Burdulis, No. 10–40003–FDS, 2011 WL 1898941 (D. Mass. May 19, 2011). Defendant in this case emailed a police officer impersonating a young boy an explicit image. Id. at *1. Police obtained a warrant to search the defendant's computer. Id. at *2. During their search of image files on the computer, police uncovered child pornography. Id. After finding the seizure of those images authorized by the initial warrant, the court held in the alternative that the plain view doctrine also authorized the use of those images in evidence. Id. at *11–12. First, the officer searching the computer was lawfully in a position to view the evidence because he was conducting a search pursuant to a warrant. Id. at *11. As he was looking for image files, he was authorized to briefly examine all images to determine if they were a match. Id. Second, by this same logic, the officer had a lawful right of access to the files. Id. at *12. Third, the prohibited nature of child pornography images would have been immediately apparent. Id. [The court did

not examine the fourth requirement—inadvertence—because it exists only under Massachusetts law. See above for more detail on inadvertence.]

(3) Exigent Circumstances

"One well-recognized exception [to the warrant requirement] applies when 'the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" Kentucky v. King, 563 U.S. 452, 460 (2011) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)). Among the exigencies that the Court has identified in the context of searching a home are "emergency aid" (entering a home to render assistance to an injured occupant), "hot pursuit" (chasing after a fleeing suspect), and the need to prevent the "imminent destruction of evidence." Id.

- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020). Police seized defendant's phone, then answered an incoming call to the phone approximately one hour and fourteen minutes after the seizure. Id. at 437–48. The Commonwealth argued that exigent circumstances justified answering the call, but it did not offer "any evidence that it was impracticable to obtain a search warrant before the call was received." Id. at 441. The court allowed defendant's motion to suppress the call and evidence derived from it, explaining that "because there [was] no evidence in the record that obtaining a warrant was impracticable here, the Commonwealth failed to meet its burden of showing exigency, and [the court was] constrained to conclude that the motion to suppress should have been allowed." Id. at 442. The court noted, however, that the burden to show that it was impracticable to obtain a search warrant in one hour and fourteen minutes was not a heavy one and could potentially have been met by an officer's testimony about the steps necessary to obtain a warrant. Id. This case indicates that courts are unlikely to treat a "one hour or two hour time frame" as *by itself* sufficient to justify a search under exigent circumstances, id. at 439, but leaves open the possibility that the same search might have been found justified had the government produced evidence showing why that short timeframe made obtaining a warrant impracticable. Id. at 442 (but see Alvarez, 480 Mass. 1017 (2018) (holding that a police officer observing a text message on the screen of a phone that was lawfully in his custody, when he glanced at the phone because it started ringing, was not a search absent evidence of further action by the officer and absent any argument by the defendant that "observation of the outside of the… phone constituted a search")).

- Commonwealth v. Cruzado, 480 Mass. 275 (Aug. 10, 2018). Police found a cell phone lying near the defendant in a stairwell. Id. at 282. Having probable cause, the police seized the cell phone. Id. The Supreme Judicial Court held that "exigent circumstances supported the warrantless seizure: the risk of someone taking or tampering with the cell phone. Left unattended, especially in an area to which many people had access, the cell phone would have been at the risk of theft or vandalism." Id. at 283.

- Commonwealth v. Dyette, 87 Mass. App. Ct. 548 (2015). Possible degradation of a call log on a cell phone was deemed not an exigent circumstance because such degradation could be prevented in a number of different ways, such as by turning off the phone. Id. at 558–59.

- Commonwealth v. Kaupp, 453 Mass. 102 (2009). Police observed pirated movies in the publicly shared folder of one of defendant's (a teacher) computers in a school classroom. Id. at 105, 107. The publicly shared folder of a different computer nearby contained both pirated movies and child pornography. Id. at 103–05. Police seized both computers and subsequently obtained a search warrant. Id. at 105. The Court upheld the seizure of defendant's computer as appropriate because of exigent circumstances. Id. at 105–06. Specifically, the Court noted that "impoundment of an object pending the issuance of a search warrant violates the Fourth Amendment . . . only if it is unreasonable," which "turns on the facts of each case, requiring courts to 'balanc[e] the need to search or seize against the invasion that the search or seizure entails.'" Id. at 106 (quoting Commonwealth v. Catanzaro, 441 Mass. 46, 55–56 (2004)). The Court held that "[g]iven the ease with which computer files may be accessed and deleted, and the disruption that would have been created by posting an officer in the defendant's office and preventing students from entering pending the issuance of a search warrant . . . the seizure was reasonable." Id. In a footnote, the Court noted that while exigent circumstances justified the seizure, they would not have justified the subsequent search had it been warrantless because "[t]he exigency necessitating [the computer's] seizure dissipated once the computer had been secured." Id. n.7.

(4) Emergency Aid Exception

The emergency aid exception to the warrant and probable cause requirements originated in the context of searching a home, "permit[ting] the police to enter a home without a warrant when they have an objectively reasonable basis to believe that there may be someone inside who is injured or in imminent danger of physical harm." Commonwealth v. Peters, 453 Mass. 818, 819 (2009). The exception has since been extended to "uphold warrantless searches of places other than homes, in order to find and assist a victim of serious physical harm or to prevent such harm from occurring," and most recently to searches of the digital information. Commonwealth v. Raspberry, 93 Mass. App. Ct. 633, 639-40 (2018).

- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018). Police officers listening to a wiretap had "grave concerns about the defendant imminently causing serious bodily harm" to another with a firearm. Id. at 635 (internal quotation marks omitted). To locate the defendant and prevent the harm, police "asked AT&T to perform 'emergency pings' and give the police real-time CSLI about the approximate location of the defendant's cell phone." Id. The Commonwealth did not contest that a Fourth Amendment "search" took place, instead arguing that the "search" was "reasonable" under the emergency aid doctrine. See id. at 638, 640. The Massachusetts Appeals Court agreed. See id. at 641 ("We have no difficulty concluding that these standards were met here . . . What police did not know here, at the time of the call, was the whereabouts of the defendant. In the circumstances, it was objectively reasonable for the police to request real-time CSLI, in order to determine the defendant's current location and the direction in which she was moving, and thus to find and intercept her before she could shoot Dorsey.").

The emergency aid exception differs from the exigent circumstances exception: the former requires no probable cause to conduct a search, whereas the latter permits a warrantless search where probable cause exists but the circumstances make obtaining a warrant impracticable. Raspberry, 93 Mass. App. Ct. at 638, n. 8.

(5) Inventory Exception

Seizures of items on an arrestee's person may also be permissible, subject to police inventory policies. "[B]efore a person is placed in a cell, the police, without a warrant, but pursuant to standard written procedures, may inventory and retain in custody all items on the person . . . ." Commonwealth v. Seng, 436 Mass. 537, 550 (2002). For such seizure to be lawful, police must follow the rules of a written inventory policy that is "explicit enough to guard against the possibility that police officers would exercise discretion with respect to whether to open closed [containers] as part of their inventory search." Commonwealth v. Rostad, 410 Mass. 618, 622 (1991). "Inventory searches are intended to be noninvestigatory and are for the purpose of safeguarding the defendant's property, protecting the police against later claims of theft or lost property, and keeping weapons and contraband from the prison population." Barillas, 484 Mass. at 256. As such, "[i]n making an inventory — taking from the person, noting what is received, and placing it in safekeeping — the police are to act more or less mechanically, according to a set routine, for to allow then a range of discretion in going about a warrantless search would be to invite conduct which by design or otherwise would subvert constitutional requirements." Commonwealth v. Sullo, 26 Mass. App. Ct. 766, 772 (1989) (cited in Barillas, 484 Mass. at 259).

Investigatory use of items seized under the inventory exception is impermissible unless the police have a search warrant or "obtain consent from the appropriate person (as determined by the inventory policy)." Barillas, 484 Mass. at 257. Any evidence resulting from investigatory use of inventory items without consent or a warrant is subject to suppression. Id.

- Commonwealth v. Mauricio, 477 Mass. 588 (2017). Defendant was arrested in connection with a breaking and entering. Id. at 589. Police conducted an inventory search of his backpack and found a digital camera. Id. at 589–90. Believing the camera to be stolen, police turned it on and looked at the images stored on it in order to identify the owner. Id. at 590. One of the images depicted the defendant holding a firearm later confirmed to have been stolen in a separate break-in. Id. The image was used to convict the defendant of carrying a firearm without a license. Id. at 589. The SJC rejected the argument that the search of the camera was a valid inventory search, holding that it was instead investigatory in nature because the camera was suspected stolen and the search was meant to identify the owner. Id. at 595–96.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found the defendant hiding in his home, conducted a pat frisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to

unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. Id. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure of the phone was lawful under the search incident to arrest exception. Id. at 255. However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Id. at 258-59. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

(6) Consent

Warrantless searches are permissible with appropriate advance consent.

- Commonwealth v. Barillas, 484 Mass. 250 (2020). Defendant was arrested on outstanding warrants after a tip connecting him to a murder. Id. at 250. Police found defendant hiding in his home, conducted a patfrisk, and seized a cellphone from defendant's shorts pocket. Id. They took the defendant to the police station, along with his father Eduardo and 13-year-old brother James, who agreed to come along to be interviewed. Id. at 251–52. At the police station, James told the police that the cellphone they had seized belonged to him. Id. at 252. To check this claim, the police asked James for the code to open the cellphone: James provided it and it worked to unlock the phone. Id. The police then presented a voluntary consent to search form for the device, which James and Eduardo signed. A police officer immediately searched the phone and discovered a video of the defendant talking about the crime. Id. "A later forensic search revealed evidence of calls and text messages between the victim and the defendant on the night of the stabbing." Id. Defendant's motion to suppress all evidence derived from the cellphone's warrantless seizure and search was granted because "the seizure of the cell phone was proper but the search of the cell phone was not." Id. at 254. The court held that the seizure was lawful under the search incident to arrest exception. Id. at 255.However, the search was improper because the police "made investigative use of the cell phone" during the conversations with James at the police station before obtaining consent to search the phone. Even if the police officer was at first "only attempting to establish ownership of the cell phone, the search exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception" Id. at 259 (quotations and citations omitted).

- Commonwealth v. Fredericq, 482 Mass. 70 (2019). The defendant, charged with trafficking cocaine, successfully sought to suppress CSLI data tracking the cell phone location of the driver of the car in which he was riding. Id. at 71. The Court held that the defendant had standing to challenge the CSLI search because he was "a passenger of the vehicle whose location was effectively being continually tracked through CSLI monitoring," and had a reasonable

expectation of privacy in his movements. Id. at 77. The Court further held that the consent search of the defendant's residence was tainted by the illegal CSLI search. Id. at 71. Believing that the defendant and a second individual were transporting narcotics from Florida to Massachusetts, police obtained a court order pursuant to 18 U.S.C. § 2703 (2006) requiring the second individual's cellular service provider to "ping" the location of his cell phone. Id. at 73-74. After the two returned to Massachusetts, police knocked on the defendant's door and told him they knew he had just "purchased a large amount of narcotics" in Florida and was possibly storing it at his apartment. Id. at 74. The defendant then consented to a search, and police discovered a large amount of cash and two bricks of cocaine in his residence. Id. at 75. The SJC considered three factors in determining whether the defendant's consent was attenuated from the tainted CSLI data: "(1) the amount of time that elapsed between the defendant being confronted with the illegally obtained CSLI evidence and his grant of consent; (2) the presence of any intervening circumstances during that time period; and (3) the purpose and flagrancy of the official misconduct." Id. at 81-82 (internal quotes omitted). As to factors (1) and (2), the Court held that the lack of time and intervening events between the acquisition of the CSLI data and the police officer's confrontation with the defendant claiming that he had just returned from Florida with drugs weighed heavily against attenuation. Id. at 82-83. As to factor (3), while the Court "recognize[d] that the illegal police misconduct here was neither purposeful nor flagrant," it was still not dispositive in attenuating defendant's consent from the tainted CSLI data. Id. at 84. In her dissent, Justice Cypher explained that she would not reach the conclusion of the majority that a passenger in a tracked car has standing to challenge a CSLI search. Id. at 86 n.1 (Cypher, J., concurring in part and dissenting in part). In addition, she encouraged the SJC to adopt the good faith exception to the exclusionary rule in cases where the police acted under a "reasonable good faith belief that their conduct was lawful at the time." Id. at 92. While Justice Lowy agreed that Massachusetts should adopt a good faith exception, he did not believe the issue was properly raised by the Commonwealth in this case. Id. at 85-86 (Lowy, J., concurring).

3. The Exclusionary Rule

Generally, the exclusionary rule prohibits the introduction of evidence obtained as a result of a violations of the Fourth, Fifth and Sixth Amendments to the U.S. Constitution, and their counterparts under the Massachusetts Declaration of Rights. See Commonwealth v. Lora, 451 Mass. 425, 439 & n.26 (2008).

a) Good Faith / Substantial and Prejudicial

The Supreme Court has limited the application of the exclusionary rule in federal cases where officers acted in good faith, but Massachusetts does not recognize the good faith exception under art. 14. See Commonwealth v. Porter P., 456 Mass. 254, 273 (2010). Instead, it looks to "the foundational purpose of the rule—to deter unlawful police conduct . . . as a guiding principle" to determine whether evidence should be excluded. Commonwealth v. Maingrette, 86 Mass. App. Ct. 691, 697 (2014) (citing Commonwealth v. Wilkerson, 436 Mass. 137, 142 (2002)). Where:

> an arrest is wrongly made on the basis of mistaken information chargeable solely to the police, the burden is on the government to show . . . that the [government's] mistake was reasonable in the circumstances, and that the violation was minor or insubstantial and nonprejudicial and that exclusion of the evidence would not be likely to deter future police misconduct.

Id. (citations omitted).

b) Inevitable Discovery

> "Under the inevitable discovery doctrine, if the Commonwealth can demonstrate by a preponderance standard that discovery of the evidence by lawful means was certain as a practical matter, the evidence may be admissible as long as the officers did not act in bad faith to accelerate the discovery of evidence, and the particular constitutional violation is not so severe as to require suppression."

Commonwealth v. Fontaine, 84 Mass. App. Ct. 699, 709 (2014) (citation omitted). Though there are no Massachusetts cases applying this doctrine to a computer search, the First Circuit case below applying a slightly different federal test is instructive:

- United States v. Crespo-Rios, 645 F.3d 37 (1st Cir. 2011). In this case, the FBI searched the defendant's computer and external hard drive for evidence of chats between both him and an undercover agent and him and minors. Id. at 40–41. The search for these chats was conducted pursuant to a warrant that also listed, among other things, child pornography as something being sought. Id. at 40. During this search, agents found child pornography. Id. Following his indictment, the defendant moved to suppress the evidence, arguing that there was insufficient probable cause to support the overly-broad search warrant. Id. at 41. The First Circuit overturned the lower court by applying the inevitable discovery doctrine. Id. at 42-44. In searching the computer and hard drive for the chat evidence—for which there was undoubtedly probable cause—the court found that government agents would inevitably have discovered the child pornography because searching for computer files allows brief scanning of all possibly relevant files on the computer. Id. [This analysis is quite similar to that of the plain view doctrine, discussed elsewhere in this guide.]

B. Search of Electronic Service Providers

1. General Overview of Stored Communications Act

In 1986, Congress enacted the Stored Communications Act (SCA). See Pub. L. 99-508, 100 Stat. 1848, Title II. It provides limited privacy protections to the customers of "electronic communication service[s]" (ECS) and "remote computing services" (RCS). Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 383 (2014). ECS providers are email services like Gmail or Yahoo! along with certain elements of social media platforms, like a user's Facebook "wall." See generally Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 8–11 (2013).

RCS providers are harder to define and include any company that provides "computer storage or processing services by means of" the Internet to the public. Pub. L. 99-508, 100 Stat. 1848, § 2710. Cloud storage providers like Dropbox clearly fit this definition. Jeffrey Paul DeSousa, Self-Storage Units and Cloud Computing, 102 Geo. L.J. 247, 250 n.19 (2013). Courts have also found that YouTube belongs in this category. Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service 11 (2013).

For a discussion of the argument that text messaging services are "remote computing services" under 18 U.S.C. § 2703(b) see Commonwealth v. Fulgiam, 477 Mass. 20, 31–33 (2017). The SJC held that the Commonwealth may not obtain the content of text messages without a warrant because text messaging is an "electronic communication service" subject to the requirements of § 2703(a). Id. at 32–33. The SJC also decided that a warrant supported by probable cause was also required for the content of text messages under art. 14. Id. at 33–34.

2. Search warrants served on out-of-state Internet service providers

Out-of-state corporations providing ECS or RCS to Massachusetts residents are subject to the jurisdiction of Massachusetts courts and must comply with search warrants issued by them. See Mass. Gen. Laws ch. 276, § 1B (2018); see also 18 U.S.C. § 2703 (2018) (outlining process by which state courts exercise jurisdiction over ECS and RCS providers).

C. Encryption and Self Incrimination

1. The Foregone Conclusion Doctrine

The Fifth Amendment to the United States Constitution states, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." This does not mean that a defendant cannot be compelled to produce some types of incriminating evidence, however, because only compelled *testimonial* communication that incriminates is barred. See Commonwealth v. Gelfgatt, 468 Mass. 512, 519 (2014) (citing Fisher v. United States, 425 U.S. 391, 408 (1976)). Written or oral communication created in response to government demand is plainly testimonial. See id. at 520. Compelled action that communicates something can also be testimonial in nature. Id.

"Whether an act of production is testimonial depends on whether the government compels the individual to disclose 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Gelfgatt, 468 Mass. at 520 (quoting United States v. Hubbell, 530 U.S. 27, 43 (2000)). For example, giving blood, producing a voice exemplar, or standing in a lineup are all nontestimonial because the suspect in question "is not required to disclose any knowledge he might have, or to speak his guilt." Id. at 521 (citations omitted). By contrast, complying with the government's demand could be testimonial "where [the act of production] is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence." Id. (citing Hubbell, 530 U.S. at 36 & n.19).

Even in cases where the act of producing evidence that the government seeks to compel is testimonial, however, that production loses its testimonial character if the information that would be

disclosed by the production is a "foregone conclusion." Id. at 522. The forgone conclusion exception obtains "where the facts conveyed already are known to the government, such that the individual 'adds little or nothing to the sum total of the Government's information.'" Id. (quoting Fisher, 425 U.S. at 411). In other words, "the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production." Commonwealth v. Jones, 481 Mass. 540, 547 (2019).

Several State and Federal courts have "applied the foregone conclusion exception in the context of compelled decryption," but neither the United States Supreme Court nor the Circuit Courts of Appeal have ruled on the government's burden of proof that applies to the "foregone conclusion" exception under the Fifth Amendment. Jones, 481 Mass. at 550. One federal district court "concluded that the appropriate standard of proof under the Fifth Amendment is clear and convincing evidence. Id. (citing United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018).

- In re a Grand Jury Investigation, 92 Mass. App. Ct. 531 (2017). During a grand jury investigation, a judge ordered petitioner to enter his personal identifying number (PIN) access code into his iPhone smartphone. Id. at 532. A warrant had previously issued for a search of the phone. Id. The Appeals Court held that production of the PIN was within the foregone conclusion exception to the Fifth Amendment. Id. at 534. To meet its burden under the doctrine, the prosecution had to demonstrate knowledge of the ownership and control of the cell phone and its contents, as well as "knowledge of the fact of [PIN code protection], and knowledge of the [existence of the PIN code]." Id. (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 524 (2014)). The prosecution was not required to show that it knew the specific content of the cell phone, but it did need to demonstrate knowledge of the existence and the location of the content. Id.

Article Twelve (art. 12) of the Massachusetts Declaration of Rights—analogous to the Fifth Amendment—provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself." Article Twelve provides greater protection than the Fifth Amendment in some contexts, but this broader protection "does not change the classification of evidence to which the privilege applies," so only "testimonial or communicative" evidence is protected from compelled disclosure. Commonwealth v. Gelfgatt, 468 Mass. 512, 525 (2014) (citations omitted). Massachusetts also recognizes the "foregone conclusion" exception to art. 12. Id. at 526.

For the exception to apply in the context of an order compelling decryption of an electronic device, Article Twelve requires that "the Commonwealth . . . prove beyond a reasonable doubt that the defendant knows the password." Commonwealth v. Jones, 481 Mass. 540, 552. But the Commonwealth does not need to "prove any facts with respect to the contents" of the device to be decrypted. In addition, "the entry of the password alone does not convey the fact of 'ownership' of the device or its contents." Id. at 547 n.8.

2. Encryption

In an affidavit the Commonwealth submitted in Gelfgatt, the director of the Massachusetts Attorney General's computer forensics laboratory explained that "encryption" is:

> the process by which 'readable' digital media, that is, digital media or data that can be viewed and accessed, is scrambled in such a way as to render that digital media or data 'unreadable' without decryption. Encryption can be performed both by hardware and by means of software tools.

Commonwealth v. Gelfgatt, 468 Mass. 512, 516 n.9 (2014). The director described "decryption" as:

> the process by which encrypted, scrambled data is rendered 'readable' again. In order to decrypt data, the person seeking decryption performs some action such as the entering of a password, scanning of a fingerprint or [insertion of] a USB Thumb drive with a pass code key on it. The encryption software then translates this action into a 'key,' essentially a string of numbers or characters. The encryption software then applies this key to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again.

Id. In Gelfgatt, the Commonwealth represented that the defendant's encryption software was virtually impossible to decrypt. Id. at 516–17. The Commonwealth represented that files thus encrypted could only be viewed if an authorized user entered a password. Id. at 517. But compelling the user to enter or disclose their password presents a possible violation of the Fifth Amendment and art. 12. The Gelfgatt court examined the interplay of these issues in Massachusetts:

- Commonwealth v. Gelfgatt, 468 Mass. 512 (2014). Defendant in this case was allegedly involved in a mortgage fraud scheme. Id. at 513. Law enforcement believed proof of that scheme would be found on the defendant's computers, and they obtained a search warrant, but encryption on the computers foiled their search. Id. at 516–17. When interviewed by police, the defendant admitted to owning multiple computers, stated that the police would be unable to access them because they were encrypted, and stated that he was able to decrypt the computers but refused to do so. Id. at 517. The lower court found that compelling him to do so would violate his Fifth Amendment and art. 12 rights against self-incrimination. Id. at 518–19. The SJC reversed and held that he could be compelled to enter his password in the circumstances presented by this case. Id. at 519–26.

  > First, the Court stated that compelling a defendant to enter a decryption password, in the abstract, implicated the Fifth Amendment because the defendant would be implicitly "acknowledging that he has ownership and control of the computers and their contents," which could itself be relevant to the Commonwealth's case against him. Id. at 522. Next, the Court considered the "foregone conclusion" exception (explained above) and held that it applied because the defendant had already admitted to owning multiple computers, that their contents were encrypted, and that he was capable of decrypting them. Id. at 523-24. As a result, the facts that would have been communicated by compelling him to decrypt the computers were already known to the government,

making them a foregone conclusion. Id. Finally, the Court examined the issue under art. 12 but held that the same analysis applied. Id. at 524–26. [Note: Crucially, the Commonwealth proposed a protocol for decrypting the files that limited the scope of what was communicated through the compelled decryption. That protocol is outlined above.]

- Commonwealth v. Jones, 481 Mass. 540 (2019). Defendant was charged with trafficking a person for sexual servitude, Mass Gen. Laws ch. 265, § 50(a) (2018); id. at 541, and deriving support from the earnings of a prostitute, Mass. Gen. Laws ch. 272, § 7 (2018); id. at 541. The Commonwealth seized an LG cell phone from the defendant at his arrest and later obtained a warrant to search the phone. Id. at 541, 544. The LG phone had to be decrypted with the entry of a password before the search could be executed. Id. at 541. The Commonwealth moved for a Gelfgatt order, compelling the defendant to decrypt the LG phone under the "forgone conclusion" exception to the privilege against self-incrimination under the Fifth Amendment to the U.S. Constitution and Article 12 of the Massachusetts Declaration of Rights. Id. at 541–42. The SJC found that in order to obtain a Gelfgatt order compelling a defendant to decrypt an electronic device, the Commonwealth must "prove that the defendant knows the password beyond a reasonable doubt for the foregone conclusion exception to apply." Id. at 542–43. The Court also concluded that the Commonwealth met its burden in this case. Id. at 543. Finally, the SJC concluded that judges can consider new information in deciding renewed Gelfgatt motions, "without first finding that [the new information] was not reasonably available to the Commonwealth at the time the earlier Gelfgatt motion was filed." Id.

  To meet its burden of proving beyond a reasonable doubt that the defendant's knowledge of the password was a "foregone conclusion," the Commonwealth offered the following evidence: a witness testified to the defendant's regular use of the LG phone to answer calls and communicate through text messages (the record revealed several communications between the witness's phone and the LG phone related to prostitution); the defendant's phone number was listed with his name in the witness's contacts; the LG phone was in the defendant's possession at the time of arrest; the defendant had characterized the telephone number of the LG phone as his number to police when he was being booked following an arrest in an unrelated matter; police records showed that a backup number listed for the LG phone was registered to a person with the same name, social security number, and date of birth as the defendant; CSLI records revealed that the LG phone was in the same location at the same time as another phone that was found to be the defendant's phone. Id. at 556–57. All of this evidence, "taken together with the reasonable inferences drawn therefrom, prove[d] beyond a reasonable doubt that the defendant [knew] the password to the LG phone." Id. at 557 (noting that "it is hard to imagine more conclusive evidence" showing that the defendant knows the LG phone's password). The SJC also noted that even if the LG phone was used by more than one person, proof of ownership or exclusive control was not required. Id. at 547 n.8.

3. Sample Decryption Protocol

In Commonwealth v. Gelfgatt, the Commonwealth employed the following protocol to limit the amount of information that would be communicated by the compelled decryption:

> 1. The defendant, in the presence of his counsel, shall appear at the [Digital Evidence Laboratory] of Massachusetts Attorney General [Maura Healey] within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
>
> 2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
>
> 3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
>
> 4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
>
> 5. The defendant is expressly ordered not to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program;
>
> 6. The Commonwealth shall not view or record the password or key in any way; [and]
>
> 7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter.

Id. at 517 n.10.

D. Searches Implicating Attorney-Client Privilege

Searches that may intercept privileged communications between a suspect and his lawyer should be handled with special care. See generally Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 811 (2013). This problem is especially acute when a search is executed after a suspect has already been indicted and retained counsel. See, e.g., id. Even when a post-indictment search targets a different crime than the one for which the defendant was indicted, such a search runs a risk of encountering

privileged communications. Id. at 817–18. The section below detail how such a search should proceed in Massachusetts.

1. Post-Indictment Email and File Searches

The Commonwealth may seize emails of a defendant under indictment by means of an ex parte search warrant. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 821–22 (2013). Because of the sensitive nature of such a seizure, however, "only a Superior Court judge may issue a search warrant seeking e-mails of a criminal defendant under indictment." Id. at 822. The affidavit supporting the warrant application must inform the judge at the outset that the subject of the email search is under indictment and must explain the connection, if any, between the indictment and the search warrant being sought. Id. Finally, the affidavit must explain why a search warrant rather than a rule 17(a)(2) summons is necessary to obtain the emails. Id. One possible explanation the SJC has suggested is cases where the Stored Communications Act requires a warrant, which it does for emails not yet opened that are 180 or less days old. See id. at 819 n.17 (citing 18 U.S.C. § 2703(a)), 822.

Once seized, emails possibly containing privileged material may be searched only after the Commonwealth receives a Superior Court judge's approval of a search protocol including specific procedures to protect against searches of privileged communications between a defendant and his attorneys. Id. at 823. One such procedure that the Court has approved is laid out below in the "Taint Team" section.

2. Taint Teams

A "taint team" is a group of attorneys or agents employed by a government office who have not at any time been involved in the investigation and/or prosecution of the defendants and who will not be assigned to any such investigation or prosecution in the future who sort the defendant's communications into privileged and unprivileged so that the latter group may be investigated by the government without eroding a defendant's attorney-client privilege. See Preventative Med. Assocs., Inc. v. Commonwealth, 465 Mass. 810, 824–25 (2013).

There is "widespread skepticism" about the ability of government agents to properly review privileged communications without affecting that privilege, id. at 825, but the SJC has concluded that taint teams can "offer adequate protection to the Commonwealth's citizens," id. at 827. To that end, the SJC has put in place a two-tiered set of requirements surrounding the use of taint teams.

First, before a judge may authorize a team that will use members of a prosecutor's office as its members, "the Commonwealth must establish the necessity of doing so" because "use of an independent special master offers a far greater appearance of impartiality and protection against unwarranted disclosure and use of an indicted defendant's privileged communications." Id. at 829. In ruling on the prosecution's request to use a taint team, "the judge may consider factors such as the number of documents to be searched, the relative cost of a special magistrate, and the Commonwealth's unique ability to perform such a search due to specialized computer forensic examiners in its employ." Id. Further, the judge will consider "the Commonwealth's ability to erect an impenetrable wall between members of the taint team and members of the prosecution team." Id. at 829–30. In making this

determination, the judge will consider "the size of the particular prosecutor's office," and the Court expressed "less confidence that a small District Attorney's office can screen off members of the taint team as effectively as the Attorney General's office may be able to do." Id. at 830.

> Second, to pass constitutional muster, the taint team must comply with each of four requirements:
>
> (1) the members of the taint team must not have been and may not be involved in any way in the investigation or prosecution of the defendants subject to indictment—presently or in the future; (2) the taint team members are prohibited from (a) disclosing at any time to the investigation or prosecution team the search terms submitted by the defendants, and (b) disclosing to the investigation or prosecution team any e-mails or the information contained in any e-mails, subject to review until the taint team process is complete and in compliance with its terms; (3) the defendants must have an opportunity to review the results of the taint team's work and to contest any privilege determinations made by the taint team before a Superior Court judge, if necessary, prior to any e-mails being disclosed to the investigation or prosecution team; and (4) the members of the taint team must agree to the terms of the order in writing.

Id. at 828.

3. Third Parties and Attorney-Client Privilege (e.g., CC'd Emails)

"'Generally, disclosing attorney-client communications to a third party undermines the privilege.'" Dahl v. Bain Capital Partners, LLC, 714 F. Supp. 2d 225, 227 (D. Mass. 2010) (quoting Cavallaro v. United States, 284 F.3d 236, 246–47 (1st Cir. 2002)).

"'An exception to this general rule exists for third parties employed to assist a lawyer in rendering legal advice,'" including CC'ed emails. Id. at 227 (quoting Cavallaro, 284 F.3d at 247). In order for the exception to obtain, three criteria must apply: (1) the communication must be "necessary, or at least highly useful" for effective consultation between client and lawyer; (2) the exception only applies if the third party is playing an interpretive role between the lawyer and client (e.g., an accountant if he is helping the lawyer understand complex financial information); and (3) the communication must be made for the purpose of rendering legal advice, and not business advice or otherwise. Id. at 227–28.

II. Evidentiary Matters

A. Judicial Discretion

1. Trial Judge's Discretion

"A judge has broad discretion in the admission" of "demonstrative aids, including digital photographs and computer-generated images." Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing Commonwealth v. Noxon, 319 Mass. 495, 536 (1946)).

For an example of related flawed evidentiary practice, see Commonwealth v. Mienkowski, 91 Mass. App. Ct. 668 (2017). At a trial for aggravated rape of a child, posing a child in a state of nudity, and of dissemination of matter harmful to minors, the defendant's cell phone was admitted into evidence. Id. at 669. After some initial ambiguity about how the jury could examine the phone during deliberation, the judge adopted the Commonwealth's position and instructed the jury to limit their examination to the evidence already admitted (screenshots of relevant text messages). Id. at 675–77. On appeal, the defendant argued that the judge's initial admission of the cell phone without limitation and statements he made at the charge conference led defense counsel to rely in her closing on the jury's ability to examine the cell phone unconstrained and then "cut the legs out from under" her argument. Id. at 677–78. The SJC found it was possible that "neither the litigants nor the judge fully had considered the plethora of difficult issues that may be raised when a cell phone containing troves of unidentified electronic data is delivered into a jury's hands." Id. at 678. Though it held that it would have been preferable to resolve the ambiguity earlier, the SJC found no reversible error in the judge's handling of the issue. Id. at 678–69.

2. Demonstrative Photographs

"When, as here, the demonstrative photograph is generated as a digital image or video image, the judge must determine whether the image fairly and accurately presents what it purports to be, whether it is relevant, and whether its probative value outweighs any prejudice to the other party." Renzi v. Paredes, 452 Mass. 38, 52 (2008) (citing Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006)). "Concerns regarding the completeness or production of the image go to its weight and not its admissibility." Id. (citing Leneski, 66 Mass. App. Ct. at 295–96).

B. Discovery

1. Pornographic Images in Child Pornography Cases

"That forensic examination of the computer data by an expert retained by the defense is an essential component of effective assistance of counsel" in a child pornography case "is self-evident." Commonwealth. v. Ruddock, No. 08–1439, 2009 WL 3400927, at *3 (Mass. Super. Ct. Oct. 16, 2009). If an expert's access to evidence for purposes of examination is limited to the Commonwealth's facilities in order to prevent dissemination of such materials, the defendant's right to effective assistance of counsel will be unduly burdened. Id. A copy of the mirror image of a seized drive, including pornographic

images, must be given to the defendant's counsel of record and expert forensic examiner under a protective order limiting access to defense counsel and the expert. Id. (citing Mass. R. Crim. P. 14(a)(6)).

2. Wiretap transcripts

- Commonwealth v. Tavares, 482 Mass. 694 (2019). The defendant was convicted of murder in the first degree. During the investigation, police had recorded conversations between the defendant and a confidential informant using a wiretap. Id at 698. Prior to trial, the defendant moved successfully to suppress the recordings because "the investigation was not in connection in with organized crime" and thus violated G. L. c. 272, § 99. Id. at 714. After he was convicted, the defendant filed a motion for a new trial, arguing that his counsel was ineffective for failing to seek suppression of evidence derived from the recordings, as well as a "motion for postconviction discovery to obtain copies or transcripts of the wiretap recordings." Id at 714. The trial court denied both motions. Id. "Under the Massachusetts wiretap statute, a criminal defendant 'may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom' if the interception was made in violation of the statute." Id at 715 (quoting G. L. c. 272, § 99). On appeal, the SJC affirmed denial of the ineffectiveness motion, ruling that the defendant "failed to identify any specific evidence admitted at trial that was derived from the unlawful recordings." Id. But the Court reversed the denial of the motion for post-conviction discovery, concluding that the defendant is entitled to a copy of the wiretap transcript prior to any retrial. Id. at 715-716. The SJC found that the transcript would enable defense counsel to examine whether there is any improper reliance on the suppressed recordings at any future trial. Id.

3. Cell phone data

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.). The defendant, indicted on one count of rape, filed a Mass. R. Crim. P. 17(a)(2) motion to obtain information from the victim-witness's cell phone relating to her electronic communications and use of social media over a twelve-day period beginning with the day of the incident. Id. at *2–3. The motion judge ordered the victim-witness to produce her cell phone and/or any "backups" for forensic examination to recover the sought-after information. Id. at *3. The judge also ordered that the victim-witness provide the names and login information for third-party service providers that possessed the information, and directed Facebook to provide Facebook and Instagram data associated with the victim-witness's accounts, including photographs and the contents of messages. Id. The victim-witness, joined by the Commonwealth, petitioned a single justice of the Supreme Judicial Court for relief from the order under G.L. c. 211, § 3, asking that (1) the twelve-day period for which cell phone data was sought be more narrowly tailored to the time of the incident, and (2) the order be vacated insofar as it required the victim-witness to provide the names and login information for third-party service providers. Id. The single justice granted the requested relief. First, the justice summarized the Lampron requirements for a successful Rule 17 motion: relevance, admissibility, necessity, and specificity. Id. at *4. The justice then noted that Massachusetts case law had yet to address the use of Mass. R. Crim. P. 17 to obtain a victim-witness's cell phone communications or third-party service providers. Id. Observing that "individuals have significant privacy interests at stake in their cell phones," the justice concluded

that, "when ruling on a request under Rule 17 for a victim-witness's cell phone or cell phone records, the judge must include a consideration of these inherent privacy concerns." Id. The justice also examined decisions in which other state and federal courts had confronted similar issues, including a Minnesota Supreme Court decision holding that the fact that a "cell phone could contain exculpatory information was insufficient to order its production for examination." Id. at *5 (citing In re B.H., 946 N.W.2d 860, 870-71 (Minn. 2020)). Finally, the justice noted that Rule 17 "is a rule of production, not a rule of discovery." Id. After taking the above factors into account, and in light of the fact that the defendant could only speculate that relevant evidence might be obtained from the broad sweep of sought-after information, the justice granted the victim-witness's requested relief.

C. Authentication

1. Generally

To find that evidence is authentic, a judge must determine whether, by a preponderance of the evidence, there is sufficient evidence, including "confirming circumstances," to permit a "reasonable jury to conclude that this evidence is what the proponent claims it to be." Commonwealth v. Purdy, 459 Mass. 442, 449 (2011). Confirming circumstances are other facts that imply that evidence is what the proponent represents it to be. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011).

2. Photographs and Digital Images, Videos, and CDs

Authentication of photographs and videos is "typically… done through one of two means—having an eyewitness testify that the [photo or] video is a fair and accurate representation of what he saw on the day in question, or having someone testify about the [recording] procedures and the methods used to store and reproduce the [photo or] video material." Commonwealth v. Connolly, 91 Mass. App. Ct. 580, 586 (2017) (citing Commonwealth v. Pytou Heang, 458 Mass. 837, 855 (2011); Commonwealth v. Rogers, 459 Mass. 249, 267 (2011)). Digital photographs and videos are treated as equivalent to their analog counterparts. See Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294–95 (2006).

These are not the only possible ways to authenticate photo and video evidence, however. Commonwealth v. Davis, 97 Mass. App. Ct. 633, 635–36 (2020). More generally, admissibility may be established by any "evidence sufficient to support a finding that the matter in question is what its proponent claims." Mass G. Evid. § 901(a). For example, a witness may authenticate a digital photograph or video by testimony about the process used to create it and "showing that it produces an accurate result." Mass. G. Evid. § 901(b)(9).

- Commonwealth v. Davis, 97 Mass. App. Ct. 633 (2020): An officer at the scene of a crime saw a surveillance camera mounted on the outside of a nearby building, aimed at the street intersection where the crime had occurred. Id. at 635. He spoke with a resident of the building, viewed a video recording taken by the surveillance camera, and learned that the camera had been pointed at the intersection at the time of the crime. Id. Neither the resident nor the officer knew how to transfer the surveillance video recording to another medium, so Carty used his cellphone to record a video of the surveillance video recording; this cellphone video was played to the jury. Id. The following

was held sufficient to authenticate the cellphone video: the officer testified (1) that he had seen the scene that appeared in the video ("a car, with its driver's side door open, that had crashed into a pole at the intersection of Quincy Street and Baker Avenue"); (2) that the surveillance camera was aimed at the intersection in question, and (3) that still photographs also in evidence were fair and accurate representations of the scene of the shooting, where the still photographs depicted multiple vehicles and a sign that also appeared the video. Id. at 636.

- Commonwealth v. Leneski, 66 Mass. App. Ct. 291 (2006): A witness sufficiently authenticated a CD containing digital images created by a digital camera system at a convenience store where that witness testified he had "viewed the images on the computer and 'burned' the CD copy; [and] testified as to the procedure he used in the surveillance process, the copying process, and to the contents of the CD." Id. at 295.

Testimony about a photo or video that is not introduced in court, but instead is described to the jury by a witness, is subject to the admissibility conditions as the original photo or video: that is, the testimony is admissible upon establishing that the photo or video the witness saw was a fair and accurate representation of the events in question. Commonwealth v. Connolly, 91 Mass. App. Ct. at 586–87.

3. Digitally Enhanced Images and Video

The SJC has indicated that even digital photographs that have been enhanced have some use as a demonstrative aid, so long as they accurately illustrate what a witness testifies about. See Renzi v. Paredes, 452 Mass. 38, 51–52 (2008) (citing 2 McCormick, Evidence § 214 (6th ed. 2006)).

When offering digitally enhanced photographs or videos, the type of media and the manner of enhancement will be relevant. See Iacobucci v. Boulter, 193 F.3d 14, 20 (1st Cir. 1999). Objections to evidence on the grounds that it lacks a proper foundation are allowed at the discretion of the judge. Id. In Iacobucci, where the audio portion of a video was enhanced with a high quality play-back system to increase the volume, the trial judge decided that this did not destroy the video's integrity and the video was properly authenticated. Id. Several witnesses positively identified the defendants' voices on the recording, and the jury had the opportunity to evaluate the identification on their own. Id. at 20–21.

Alternatively, "[f]or digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007). In such a case, there will need to be proof that the digital enhancement process produces reliable and accurate results. Id.

4. Transcripts of Recordings

A written transcript of a recorded conversation taken from an electronic transmitting device can be authenticated where a witness testifies that the transcript is a fair and accurate representation of the recording. See United States v. Anderson, 452 F.3d 66, 76–77 (1st Cir. 2006) (citing United States v. Ademaj, 170 F.3d 58, 65 (1st Cir. 1999)). That witness does not have to be the person who transcribed the recording. Id. at 77.

5. Email

"While e-mails and other forms of electronic communication present their own opportunities for false claims of authorship, the basic principles of authentication are the same." Commonwealth v. Purdy, 459 Mass. 442, 450 (2011) (citing United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006)). Email authentication does not require expert testimony or evidence of exclusive access or password protection, although they are relevant to the jury's assessment of the weight of the evidence. See id. at 451. Where the relevance or admissibility of emails depends on whether the defendant authored the emails, the judge must "determine whether the evidence [is] sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the e-mails." Id. at 447 (citing Commonwealth v. Leonard, 428 Mass. 782, 785–86 (1999); Mass. G. Evid. § 104(b)(1)).

However, where the contents of an email do not sufficiently authenticate it, it may be properly authenticated through confirming circumstances. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–75 (2011). Confirming circumstances imply that evidence is what the proponent represents it to be. Id. at 674. For example, the following confirming circumstances were sufficient to link a defendant to emails: (1) an email revealed that the sender would meet the email recipient at a certain place and time, and the defendant then appeared in that place at the time specified; (2) the sender of that email included his telephone number and a photograph of himself. Id. at 674–75. The defendant answered a call to that number, and emailed photograph depicted the defendant. Id.

Other confirming circumstances include: (1) emails originate from an account that bears the defendant's name and that the defendant admits having used; (2) emails are found on a computer hard drive that the defendant admits owning; (3) the defendant supplies all necessary passwords to access files on the computer; (4) emails contain an attached photograph of the defendant and/or describe the unusual circumstances or traits attributable to the defendant. Purdy, 459 Mass. 442, 450–51 (2011).

"Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking website such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant. There must be some confirming circumstances sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the emails." Id. at 450 (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)); see also Griffin v. State, 419 Md. 343, 357–58 (2011) (holding that authentication of a page printed from a social networking site requires more than a showing that a picture, birth date, and location of the alleged creator exist on the profile from which the page was retrieved).

Embedded e-mails will not be excluded because of the mere possibility that they can be altered without any specific evidence showing alteration. In Safavian, when "the trustworthiness of the emails particularly those . . . . emails that are included in a chain-either as ones that have been forwarded or to which another has replied" were challenged, the district court held that the "*possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course any more than it can be the rationale for excluding paper documents (and copies of those documents)."

435 F. Supp. 2d at 41 (emphasis in original). The court added that the defendant would be entitled, however, to raise any issue of alteration with the jury. Id.

6. Chatrooms

Similar to the method of authentication by confirming circumstances allowed in the Commonwealth, "[c]ourts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. For example, in [the Pennsylvania case] In re F.P., the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert . . . . The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 556 (D. Md. 2007) (citing In re F.P., 878 A.2d 91, 93–94 (Pa. Super. Ct. 2005)).

7. Text Messages

- Commonwealth v. Alden, 93 Mass. App. Ct. 438 (2018). The victim received threatening text messages from a "telephone number [she] had used to communicate with the defendant . . . every few days for over one year." Id. at 439. The trial court held that "the Commonwealth had established by a preponderance of the evidence that the text messages were authentic" - i.e., that the messages came from the defendant. Id. at 440. The Massachusetts Appeals Court affirmed because "for over one year, [the victim] had contacted the defendant multiple times each week using the telephone number from which the threatening messages originated. When she called that number, the defendant answered. When she sent a text message to that number to arrange a meeting with the defendant, he appeared." Id. at 440–41. Moreover:

> [t]he content of the text messages reinforced their link to the defendant. It is undisputed that at the time she received the text messages, [the victim] was a witness in a pending case against the defendant. In this context, where there was evidence that the text messages directed her to "keep her [explicative] mouth shut" and "leave their personal stuff out of the courtroom" or "people [would] come after [her] if [she] went to court," it was reasonable to infer that the defendant was responsible for sending the messages.

  Id. at 441.

8. Information Available on Websites and Social Networks

Evidence available on websites presents its own problems. "Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007). "The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting." Id. (citing United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000)). In doing so, federal courts require the proponent of such evidence to show what was actually on the website, to show that the

exhibit or testimony accurately reflects that content, and to show that the content can be attributed to the owner of the site. Id. (citations omitted).

In the courts of the Commonwealth, "[e]vidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant." Commonwealth v. Purdy, 459 Mass 442, 450 (2011) (citing Commonwealth v. Williams, 456 Mass. 857, 868–69 (2010)).

Circumstantial evidence can authenticate a social network page:

- Commonwealth v. Meola, 95 Mass. App. Ct. 303, No. 18-P-83, 2019 WL 2202909 (Mass. App. Ct. May 22, 2019). The Appeals Court affirmed the Superior Court's holding that sufficient evidence in the form of "confirming circumstances" established that the defendant attached an obscene video to a communication he sent to an underage victim. Following a jury waived trial, a Superior Court judge found the defendant guilty of disseminating obscene material to a minor in violation of G.L. c. 272, § 28. Id. at *1. The Appeals Court looked to the principles established by the SJC in Commonwealth v. Purdy, 459 Mass 442 (2011) regarding authenticating digital evidence (that is not self-authenticating). First, Purdy establishes that direct evidence is not necessary to determine that a defendant sent a digital communication. Rather, a judge "may consider circumstantial evidence and look to 'confirming circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored" the electronic communication. Meola, 2019 WL 2202909 at *5 (quoting Purdy, 459 Mass. at 450). Second, under Purdy, the "mere possibility that a digital communication was fraudulently sent by someone other than the person associated with a particular social media...account from which the communication originated is not a bar to its authentication." Meola, 2019 WL 2202909 at *5. Third, common-law principles concerning authenticity are applicable to digital communications. Id. In this matter, the trial judge's decision to exclude records proffered by the prosecutor, describing user information related to the Facebook account and the sender of the video, required the Commonwealth to rely on indirect evidence to authenticate the materials. Id. at *2. The Appeals Court concluded that the following facts offered sufficient indirect evidence of authenticity: the defendant's prior association with the victim (defendant had previously lived with her and her mother); the defendant's biological relation to the victim's half-sister; and the friend request the user of the account sent to the victim. Moreover, the Court determined that the trial judge did not err in finding the communications authentic because there was no evidence to suggest that the Facebook profile photo or the self-authored obscene video were publicly available. Id. at *6. Based on these facts, the Court affirmed the trial judge's determination that the defendant "purposefully disseminated matter harmful to a minor to the victim" with full knowledge that she was a minor. Id. at *7.

- Other jurisdictions have taken a similar approach. For example, in the Texas case Tienda v. State, MySpace webpages were admissible because there was sufficient evidence on them indicating that they "were what they purported to be." 358 S.W.3d 633, 646 (Tex. Crim. App. 2012). The court stated that, "as with the authentication of any kind of proffered evidence, the

best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case." Id. at 639. The court held that there was "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the Myspace pages belonged to the appellant and that he created and maintained them." Id. at 645; see also Parker v. State, 85 A.3d 682 (Del. 2014) (holding that social media post was sufficiently authenticated by circumstantial evidence and by testimony explaining how the post was obtained); Simmons v. Commonwealth, No. 2012–SC–000064–MR, 2013 WL 674721 (Ky. Feb. 21, 2013) (holding that the print-outs of the defendant's Facebook messages were admissible because the messages were what they purported to be and the role of the judge, as a gatekeeper, was only to determine if an offering party has produced enough evidence for a reasonable jury to find authenticity).

9. Software Programs Used in Investigation

When a witness uses software to create information relevant to an investigation, that witness should testify in detail as to the nature of the tool, how the witness used it, and how it was created and maintained in order to authenticate the records. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 327 (2009) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)). In Whitlock, a police officer used a software program called ArcView, which is a computerized map that depicted the location and ownership of property within the city of Springfield. Id. at 325–26. The information provided by this software was used to show that the defendant was distributing a controlled substance within a school zone. Id. Where software provides information to a witness, for example software that measures and provides distances between real-world objects, it does not make a "statement," and therefore is not subject to the hearsay rule. Id. at 326–27.

10. GPS and Probation

The SJC has held GPS technology to be "widely used and acknowledged as a reliable relator of time and location data" under the Daubert-Lanigan standard for admission of scientific testimony. Commonwealth v. Thissell, 457 Mass. 191, 198 (2010); see also Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592-3 (1993); Commonwealth v. Lanigan, 419 Mass. 15, 26 (1994). Judges may at their discretion admit testimony that "GPS data placed the defendant in particular locations at particular times" based on data from any GPS device whose positioning method has been demonstrated to be "no more than the application of existing and scientifically-accepted GPS monitoring technology -- a technology that has been accepted as reliable." Davis, 97 Mass. App. Ct. at 640. The fact, acknowledged by an appellate court, that GPS information is "subject to variations in accuracy depending upon atmospheric conditions, intervening obstacles, or reflection of the satellite signals from buildings, windows, or cars, [goes] to the weight of the evidence, not to the fundamental reliability of the GPS technology." Id. (citing Sacco v. Roupenian, 409 Mass. 25, 30 (1980); Rothkopf v. Williams, 55 Mass. App. Ct. 294, 299 (2002)). An appellate court has distinguished and left unresolved the issue of whether GPS records are also reliable indicators of speed (as opposed to location). Id. at 641.

Probationers' GPS records have been used as evidence of a defendant's location at particular times; evidence that can be relied on to show that the defendant violated conditions of probation or was at

the scene of a crime. Thissell, 457 Mass. at 198–99; Davis, 97 Mass. App. Ct. at 639–40. Official GPS records maintained by the Commonwealth and certified by an officer having legal custody of the record may minimize concerns about authenticity, Thissell, 457 Mass. at 199 ("recommend[ing] strongly that copies of GPS records offered in future revocation proceedings be properly attested and certified by an appropriate custodial officer"), but GPS-based information may also be authenticated on other ways. Davis, 97 Mass. App. Ct. at 637 (authenticating GPS data by the testimony of a GPS device manufacturer's manager of product development).

D. Technological evidence as the basis of criminal conviction

Evidence used as the basis of a conviction must be sufficient, viewed in the light most favorable to the government, for a rational trier of fact to find the essential elements of the crime beyond a reasonable doubt. Commonwealth v. Ayala, 481 Mass. 46, 51 (2018) (citing Commonwealth v. Latimore, 378 Mass. 671, 677-78 (1979). Thus, even evidence that meets the preponderance standard required to authenticate a piece of evidence, see § II.C, supra, may not be sufficient to support a conviction. The government bears the burden of explicit proof even for facts about technology that may be well known to the trier of fact, e.g., that a password is generally required to log in to and send messages from an Instagram account. Commonwealth v. McMann, 97 Mass. App. Ct. 558, 561 (2020). Such facts are not appropriate subjects of judicial notice. Id. at 561 n.4.

- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020). Defendant was convicted of violating an abuse prevention order that prohibited him from contacting his ex-girlfriend. Id. While the order was in effect, the ex-girlfriend received an Instagram message from user "bigm617" that said "Yoooo." Id. at 559. She testified that she knew that "bigm617" was the defendant's account "because the associated account displayed pictures of the defendant, including one of him with the victim, and the victim and the defendant had previously 'liked' and commented on each other's Instagram posts." Id. The victim showed this Instagram message to a police officer, who met with the defendant later that day. Id. The defendant denied sending any message to the victim, 'wanted to show [the officer] that he never did[,]' and entered a passcode to unlock his cell phone. He then opened the Instagram application on his cell phone, and the 'Yoooo' message to the victim appeared on the screen. The officer observed that the defendant looked '[s]urprised.' Id. The appeals court held that "even assuming without deciding that the Instagram message was properly authenticated, the Commonwealth failed to… prov[e] beyond a reasonable doubt that the defendant was the person who wrote or sent the message to the victim. Although the evidence was sufficient to show that the Instagram account was the defendant's and that he could access it, there was no circumstantial evidence establishing authorship." Id. at 560. The court suggested the burden could have been met by "evidence that the message itself contained characteristics showing that the defendant wrote it, or through evidence establishing how secure Instagram accounts are and how the Instagram cell phone application works." Id. at 562.

E. Best Evidence Rule

1. Best Evidence Rule - Generally

"The best evidence rule provides that, where the contents of a document are to be proved, the party must either produce the original or show a sufficient excuse for its nonproduction." Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001); see also Mass. G. Evid. § 1002. However, what constitutes a "document" has been narrowly construed such that "[t]he best evidence rule is applicable only to those situations where the contents of a *writing* are sought to be proved." Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970) (emphasis added). Most photographs and videos depict objects rather than writings. Consequently, the best evidence rule does not typically apply, *inter alia*, to photographs or videotapes. See also Commonwealth v. Weichell, 390 Mass. 62, 77 (1983) (holding that the "enlarged photograph was a fair and accurate representation of the defendant at the time of his arrest"); Commonwealth v Leneski, 66 Mass. App. Ct. 291, 294 (2006) ("Videotapes, like photographs, are not subject to the best evidence rule."). Additionally, "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes." Leneski, 66 Mass. App. Ct. at 294.

2. Digital Images

Digital image evidence is not subject to the best evidence rule in Massachusetts because these images are not writings. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006) (citing Commonwealth v. Balukonis, 357 Mass. 721, 725 (1970)). The Leneski court held that digital images from a computer copied to a compact disk ("CD") would be considered as originals. Id. Testimony about authenticity, including how the disc was generated, the procedure used in the surveillance process, the copying process, and the contents of the CD, was deemed sufficient. Id. The Court noted that there was opportunity for cross-examination that went to the weight of the evidence on the subject of surveillance procedure and the method of storing and reproducing the data. Id.

This exception to the best evidence rule extends to images that have been transferred from a hard drive to other media such as CDs and DVDs. See id. at 294 (holding that "digital images placed and stored in a computer hard drive and transferred to a compact disc are subject to the same rules of evidence as videotapes").

3. Admission of Duplicate Evidence

> [W]here the original [of a document] has been lost, destroyed, or otherwise made unavailable, its production may be excused and other evidence of its contents will be admissible, provided that certain findings are made.
>
> As a threshold matter, the proponent must offer evidence sufficient to warrant a finding that the original once existed. . . . If the evidence warrants such a finding, the judge must assume its existence, and then determine if the original had become unavailable, otherwise than through the serious fault of the proponent . . . and that reasonable search

> had been made for it. . . . If the judge makes these findings in favor of the proponent, the judge must allow secondary evidence to establish the contents of the lost writing.

Commonwealth v. Ocasio, 434 Mass. 1, 6 (2001) (quoting Fauci v. Mulready, 337 Mass. 532, 540–43 (1958) (internal citations and quotation marks omitted)).

4. Videos

The best evidence rule does not apply to digital videos. Commonwealth v. Leneski, 66 Mass. App. Ct. 291, 294 (2006). "Our courts have held that videos are 'on balance, a reliable evidentiary resource . . . .'" Id. (quoting Commonwealth v. Harvey, 397 Mass. 351, 359 (1986)). "[Videos] 'should be admissible as evidence if they are relevant, they provide a fair representation of that which they purport to depict, and they are not otherwise barred by an exclusionary rule.'" Id. (quoting Commonwealth v. Mahoney, 400 Mass. 524, 527 (1987)).

5. Email

It is unlikely that printed email communications are subject to the best evidence rule so long as their authenticity can be proven through circumstantial evidence. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 675–76 (2011). In Amaral, the court reasoned that the email server, or the computer itself, is not better evidence than directly printed emails, and that "[t]he significance of the best evidence rule has declined appreciably in recent decades." Id. at 675 (internal quotation marks omitted).

6. Summaries

Large volumes of digital evidence may be summarized and shown to a jury without running afoul of the best evidence rule.

In the Commonwealth, voluminous evidence that would be difficult for a jury to understand due to volume or complexity may be presented in the form of a written or testimonial summary or a chart, shown by testimony to accurately reflect the contents of the underlying documents, so long as the proponent does not unfairly emphasize portions of the summarized evidence. See Mass. G. Evid. § 1006; Commonwealth v. Mimless, 53 Mass. App. Ct. 534, 538 (2002) (quoting Welch v. Keene Corp. 31 Mass. App. Ct. 157, 165–66 (1991)) ("[C]are must be taken to insure that summaries accurately reflect the contents of the underlying documents and do not function as pedagogical devices that unfairly emphasize part of the proponent's proof.") (internal quotation marks omitted); Commonwealth v. Greenberg, 339 Mass. 557, 582 (1959) ("The witness was not allowed to state deductions and inferences of his own but could state only the results of his computations from the admitted evidence."). The summarized evidence should be made available to other parties in advance of trial, and the court may order that the originals be produced in court. See Mass. Guide to Evid. § 1006.

- Commonwealth v. Suarez, 95 Mass. App. Ct. 562 (2019). The defendant, who was convicted of assault with intent to rape and other charges, challenged on appeal the introduction at trial of a six-minute compilation of video surveillance footage from before, during and after the attack, and a timeline describing parts of the videos. Id. at 566-67, 570. Since the defendant did not object at

trial, the Appeals Court "examine[d] whether any abuse of discretion in admitting the exhibits created a substantial risk of a miscarriage of justice." Id. at 570-71. The Court found the individual underlying videos could not 'be conveniently examined in court.'" Id. at 571 (quoting Mass. G. Evid. § 1006). Though the Commonwealth played portions of the videos in the courtroom, "a deliberating jury would have found it difficult to master the technology necessary to find and view the relevant parts of the videos in the jury room." Id. at 571-72. Furthermore, the Court rejected the defendant's claim that the compilation was unfairly edited. Id. at 572. However, the Court did find certain improprieties in the compilation and timeline. In particular, it ruled that still photos, taken from a 7-Eleven store four hours after the attack, should not have been included in the compilation because the photos taken hours after the assault were not relevant to the crime itself. Id. The Court also ruled that the timeline describing the digital compilation "could and should have used a neutral heading" for a set of video clips. Id. at 574. The Court criticized the Commonwealth's use of the term "suspect" in the timeline to refer both to a person the defendant admitted was him, in certain video clips, and to the attacker, in other video clips, since use of that term suggested that they were the same person. Id at 573. The Court ruled, however, that these "limited errors in the compilation and the timeline" did not create a substantial risk of a miscarriage of justice because they had little, if any, impact on the case. Id. at 574.

F. Hearsay

When software merely provides information to a witness, the software does not make a "statement," and therefore is not subject to the hearsay rule. See Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326–27 (2009) (holding that information provided by measuring software that indicated to the witness the distance between real-world objects were not statements subject to the hearsay rule) (citing Commonwealth v. Sheldon, 423 Mass. 373, 377 (1996)); see also Thissell, 457 Mass. at 197 n.13 (discussing the difference between computer-generated and computer-stored records in the context of the rule against hearsay); Commonwealth v. Royal, 89 Mass. App. Ct. 168, 171–72 (2016) (treating "computer-stored" records as hearsay, but treating "computer-generated" records as not hearsay); Commonwealth v. Woollam, 478 Mass. 493, 498 (2017) (holding that call logs are computer-generated records that do not raise hearsay concerns; admissibility thus only depends on authentication); Davis, 97 Mass. App. Ct. at 641–43 (holding that GPS logs and maps of the defendant probationer's location over time, which were created by a mapping company that added dots and the defendant's name to maps based on GPS location data, were not hearsay).

G. Business Records Exception

1. Email

A document from an email service provider that indicates that a specific login name is connected to a defendant's email address is admissible as a business record as long as it is supported by an affidavit from the service provider's custodian of records. Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 673–74 (2011).

2. Computer Records

"[C]omputer records . . . are admissible under the business records exception to the hearsay rule, [Mass. Gen. Laws ch.] 233, § 78, if they were (1) made in good faith; (2) made in the regular course of business; (3) made before the action began; and (4) [it was] the regular course of business to make the record at or about the time of the transaction or occurrences recorded." McLaughlin v. CGU Ins. Co., 445 Mass. 815, 819 (2006) (quoting Beal Bank, SSB v. Eurich, 444 Mass. 813, 815 (2005) (internal quotation marks omitted)).

A lack of personal knowledge on behalf of the affiant, the maker, or custodian of records goes to the weight and not the admissibility of the business records. See Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674 (2011) ("[T]he personal knowledge of the entrant or maker affects only the weight of the record, not its admissibility.") (quoting and citing Note to Mass. Guide to Evid. § 803); see also McLaughlin, 445 Mass. at 819 (2006) ("[P]ersonal knowledge of the entrant or maker of a record is a matter affecting the weight rather than the admissibility of the record.").

A print-out of an electronic document is admissible as a business record as long as it is supported by an affidavit from the provider's custodian of record establishing that the requirements of the business records exception are met. Amaral, 78 Mass. App. Ct. at 673–74 n.4; McLaughlin, 445 Mass. at 8199 ("The affidavits plainly establish that the records satisfy these foundational requirements.").

H. Confrontation Clause

1. Software-generated information

"The confrontation clause bars the admission of testimonial out-of-court statements by a declarant who does not appear at trial unless the declarant is unavailable to testify and the defendant had an earlier opportunity to cross-examine him." Commonwealth v. Wilson, 94 Mass. App. Ct. 416, 417 n.1 (2018), (quoting Commonwealth v. Simon, 456 Mass. 280, 296 (2010).

When introducing software-generated information that is not hearsay as evidence, see § II.E, supra, the Confrontation Clause is not implicated. See Commonwealth v. Hurley, 455 Mass. 53, 65 n. 12 (2009) ("admission of a testimonial statement without an adequate prior opportunity to cross-examine the declarant… violates the confrontation clause only if the statement is hearsay…") (citing Crawford v. Washington, 541 U.S. 36, 59-60 & n. 9 (2004).

It is unclear whether the introduction of software-generated information that *is* hearsay (if that is possible at all) would implicate the Confrontation Clause. An appellate court has considered the question in dicta, and suggested that (1) software-generated information may not come from a "declarant" within the meaning of the Confrontation Clause at all, but (2) if a company involved in producing the information were treated as a declarant, then the requirements of the Confrontation Clause could be satisfied by having a representative of the company as a witness. Davis, 97 Mass. App. Ct. at 644.

2. Secondary Examiners

The Sixth Amendment's bar on the testimonial statements of a witness who does not appear at trial applies to forensic examiners because their explanation of the process and results of specific forensic examinations are testimonial statements. See United States v. Soto, 720 F.3d 51, 58–60 (1st Cir. 2013) (summarizing relevant Supreme Court cases).

A "surrogate" witness who is familiar with a lab's practices, but who has formed no independent opinion of the results is insufficient to satisfy the Sixth Amendment. Id. at 58 (citing Bullcoming v. New Mexico, 564 U.S. 647, 662–63 (2011)).

However, "[t]he government may ask an agent to replicate a forensic examination if the agent who did the initial examination is unable to testify at trial, so long as the [testifying] agent . . . conducts an independent examination and testifies [as] to his own results." Id. at 59; see, e.g., Commonwealth v. Chappell, 473 Mass. 191, 199–200 (2015) (substitute DNA expert testimony allowed because, as the second reader, she independently read all the raw data and the reports produced by the original analyst, made interpretations, and ensured that there was agreement between her findings and those the analyst, and therefore testified to her opinions or conclusions concerning the DNA).

- Commonwealth v. Seino, 479 Mass. 463 (2018). Defendant was convicted of first-degree murder. Id. at 464. On appeal, he asserted several confrontation claims. Id. at 466, 469–72. First, the defendant argued that it was improper for a doctor who did not perform the autopsy to refer during his trial testimony to statements in the autopsy report and death certificate, neither of which the testifying doctor authored. Id. at 466. The SJC held that it was appropriate for the testifying doctor to offer his opinion on the cause of death based on the case file and his own examination, but agreed with the defendant that the doctor should not have testified about statements in the autopsy report and death certificate. Id. at 466–67. The SJC found that the error was harmless beyond a reasonable doubt, however, because the improper testimony was cumulative, did not incriminate the defendant, and "did not contribute to the guilty verdicts." Id. at 467–68. Second, the defendant argued that his confrontation right was violated when two experts, as part of their trial testimony, used charts showing DNA testing data obtained by other analysts (who did not testify). Id. at 469–70. The SJC held that the data should not have been shown to the jury. Id. at 470. The Court also concluded, however, that there was no substantial likelihood of a miscarriage of justice "because the charts did not taint the analysts' independent opinions, which . . . were properly admitted." Id. at 471. [Note: The Court applied a miscarriage of justice standard because the defendant did not preserve an objection to the charts at trial. Id. at 470.] The SJC noted that the charts "merely displayed genetic locations, not any information regarding a match or the statistical probability thereof." Id. at 471. Third, the defendant argued that it was reversible error for an analyst to testify that the defendant's DNA profile matched a DNA profile developed by a different analyst from the victim's jeans. Id. The SJC rejected this claim, finding that the defendant had had the opportunity at trial to cross-examine the analyst who developed the defendant's DNA profile, the supervisor of the laboratory that developed the DNA profile from the jeans, and the analyst who compared the two profiles. Id. at 471–72.

- Commonwealth v. Scesny, 472 Mass. 185 (2015). An autopsy report and photographs from the victim's autopsy were introduced in evidence and a substitute medical examiner testified regarding findings in the report. Id. at 196–97. The SJC held the autopsy report was "'inadmissible hearsay whose admission violate[s] the defendant's right of confrontation under the Sixth Amendment to the United States Constitution,'" id. at 197 (quoting Commonwealth v. Emeny, 463 Mass. 138, 145 (2012)), and that a substitute medical examiner cannot testify about the facts and findings of the report on direct examination. Id. The autopsy photographs were properly admitted through a State police trooper who attended the autopsy. Id. at 198 n.25.

- Commonwealth v. Jones, 472 Mass. 707 (2015). At defendant's trial for rape, a chemist at the State police crime laboratory, who was not present during the "rape kit" examination and had no apparent connection to the hospital at which the swabs were taken, was allowed to testify on direct examination to her "understanding" of how the swabs had been collected. Id. at 711–12. The SJC held that allowing an expert witness who had not been present during the examination and had no apparent connection to the hospital where the examination occurred, to testify on direct examination to her "understanding" of how the swabs had been collected violated the defendant's confrontation right. Id. at 708. The SJC found that the "surrogate" expert's statements were testimonial for two main reasons: (a) in labeling the various swabs and completing the "rape kit" inventory list, the initial examiner made factual statements concerning how the swabs were collected, and (b) the purpose of a "rape kit" is to gather forensic evidence for use in a criminal prosecution,. Id. at 714. These statements would therefore only be admissible if they complied with the test established by Commonwealth v. Greineder, 464 Mass. 580, 593 (2013). Id. at 715. The Jones Court summarized the holding of Greineder as follows: "'[e]xpert opinion testimony, even if based on facts and data not in evidence, does not violate the right of confrontation, provided that the facts and data 'are independently admissible and are a permissible basis for an expert to consider in formulating an opinion,' and that two further conditions are met. First, the expert must 'not present on direct examination the specific information on which he or she relied'; second, the expert witness must have the capacity to 'be meaningfully cross-examined about the reliability of the underlying data.'" Id. at 713 (quoting Greineder, 464 Mass. 580) (other citations omitted). The statements in Jones did not meet either of these requirements in Greinder: (1) the underlying hearsay facts of how the swabs were collected came in on direct examination and (2) the expert could not meaningfully be cross-examined about the reliability of the representations of the "rape kit" examiner concerning the origins of the swabs and lacked the capacity to address chain of custody and evidence-handling protocols relevant to the process by which the swabs were collected. Id. at 715–16. The testimony thus failed to comply with Greineder and was therefore inadmissible. Id. at 715.

III. Cybercrimes

A. Possession of Child Pornography

1. Multiple Convictions Require Multiple "Caches"

In prosecuting possession of child pornography, each "cache" of pornography counts as one unit of prosecution. See Commonwealth v. Rollins, 470 Mass. 66, 73–75. That is, "a defendant's possession of a single cache of one hundred offending photographs in the same place at the same time gives rise to a single unit of prosecution pursuant to [Mass. Gen. Laws ch. 272,] § 29C" rather than one-hundred separate charges and convictions. Id. at 74. To support multiple prosecutions for possession of child pornography in compliance with the Double Jeopardy Clause, that possession must be "'sufficiently differentiated by time, location, or intended purpose.'" Id. at 73 (quoting Commonwealth v. Rabb, 431 Mass. 123, 130 (2000) (with internal quotation marks omitted)).

- Commonwealth v. Wassilie, 482 Mass. 562 (2019). The defendant, who was convicted on 15 separate indictments relating to secretly videotaping nude or partially nude adults and children, appealed, arguing that the judge erred in ruling that the proper units of prosecution were the individual victims rather than the individual episodes of surveillance. Id. at 563. The defendant concealed his cell phone in a unisex, one room bathroom without stalls at an angle that gave a clear view of the toilet. Id. at 563-564. He recorded two videos on the same day, and these videos captured "genitalia of children and adults, male and female"—a total of seventeen adults and five juveniles. Id. On appeal, the Court cited precedent that, for the purpose of determining whether particular conduct constitutes a single offense or multiple offenses, there are two categories of statutes. Id. at 567. "One category is focused upon the prevention of violence or physical injury to others." Id. In this category, a single incident can give rise to multiple indictments, based on the number of victims. Id. The other category is directed at "punishing the defendant for conduct offensive to society." Id. For this second category, separate indictments for separate victims are not appropriate. Id. at 568. Some crimes, like the one at issue here, do not fit neatly into either category. Id. The defendant argued that the statute reflects an intent to punish the physical act of recording, but the Court read the statute as punishing criminal acts that invade an individual's privacy. Id. The Court also rejected the defendant's reasoning on the grounds that his statutory interpretation would produce the "absurd result" of allowing people who take illicit photos of multiple people to be tried as if they had one victim. Id. at 571. Based on this statutory analysis, the Court upheld the lower court's decision to use a per victim unit of prosecution. Id. at 578.

2. Brief Possession is Sufficient

Brief possession of offending images is sufficient to sustain a violation of Mass. Gen. Laws ch. 272, § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 329–30 (2011). Evidence of prolonged or continued control is not needed. Id. (citing Commonwealth v. Harvard, 365 Mass. 452, 458 (1969)). In Hall, although the defendant's cell phone no longer contained child pornography and though there was no confirmation that the defendant had viewed the pictures sent to him by the victim, the defendant was

found guilty of possession of child pornography because the fact that he had enticed and encouraged the victim combined with the fact that he received the images allowed a jury to find that he had possessed them. Id. at 327–29.

3. Receipt by Cell Phone is Sufficient

Confirmation that defendant's cell phone received picture messages from the victim, where the defendant enticed the victim to take and send the picture messages, is sufficient to show control and possession of such photos in violation of Mass. Gen. Laws ch. 272 § 29C. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 327–29 (2011).

4. Malware and Computer Viruses Defense

The First Circuit notes that "we must be cognizant of 'the prevalence and sophistication of some computer viruses and hackers that can prey upon innocent computer users' by placing child pornography on their machines, but 'the specter of spam, viruses, and hackers must not prevent the conviction of the truly guilty.'" United States v. Rogers, 714 F.3d 82, 87 (1st Cir. 2013) (quoting United States v. Pruitt, 638 F.3d 763, 766–67 (11th Cir. 2011)). In Rogers, the possibility that the child pornography found on the defendant's computer was a result of malware was ruled out by forensic analysis (where an analyst installed the same malware on another computer and no child pornography was found) and corroborating evidence (child pornography found on another computer, browsing history matching an interest in child pornography, and evidence that some of the pornography had been deleted by the defendant). Id.

5. Probable cause / Staleness in Child Pornography Cases

- Commonwealth v. Guastucci, 486 Mass. 22 (2020). The defendant, charged with two counts of possession of child pornography, sought to suppress evidence seized from his laptop computer and flash drive. Id. at 25. He argued that the probable cause in the affidavit in support of the warrant to search his home was stale. Id. In Guastucci, police were investigating the upload of a single image of child pornography from the defendant's home to Skype seven months prior to the search. Id. Addressing the issue of staleness in the context of a search for evidence of child pornography for the first time, the Court found that "the information in the warrant affidavit was not stale when the warrant was filed," while noting that the seven-month delay "may be at the outer limit in these circumstances." Id. at 27. Generally, "the determination of staleness in investigations involving child pornography is unique" because "individuals who are interested in child pornography are likely to collect and retain such images." Id. at 29 (quotations and citations omitted). Relying on United States v. Raymonda, 780 F.3d 105 (2d. Cir. 2015), the Court separately identified several factors for determining that a suspect is a collector of child pornography, such as: "an admission or other evidence identifying the individual as a pedophile; paid subscriptions to child pornography sites or participation in peer to peer file sharing; and a past history of possessing or receiving child pornography." Id. at 31. Further, a single incident of possession or receipt of child pornography could also lead to a reasonable inference that a suspect is interested in it, "where, for example, the images were obtained through 'a series of sufficiently complicated steps' suggesting a 'willful intention to view the files,' or where the suspect redistributed the file to others." Id. at 31 (quoting Raymonda, 780 F. 3d at 115). Here, the warrant

affidavit alleged that the defendant "uploaded an image of child pornography to an Internet chat, talk, and file-share service [Skype]", an act that required multiple, intentional steps. Id. at 32. In such circumstances, the seven month delay between the upload and the warrant application did not render the warrant stale. Id. at 27.

B. Statutory Terms of Mass Gen. Laws ch. 272

1. "Dissemination"

"The definition of 'disseminate' includes 'publish, produce, print, manufacture, distribute, . . . exhibit or display.' The statutory emphasis is on the content of the material and the intent of the person disseminating such material; the draftsmen were not so much concerned with the manner in which the image was distributed, exhibited, or displayed. The statutes criminalize such dissemination whether accomplished by way of hand, mail, facsimile, or through the use of e-mail. The judiciary ought, absent constitutional inhibitions, give effect to the purpose of the law gleaned from the Legislature's choice of language." Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *2 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 31 (internal citation marks omitted)).

"Possession" is not an element of the crime of "dissemination." Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *4 (Sep. 22, 2016) (unpublished). To "disseminate" is defined as 'to import, publish, produce, print, manufacture, distribute, sell, lease, exhibit or display." Id. at *5 (quoting Mass. Gen. Laws ch. 272, § 31). In Moore, the appeals court held that "[t]o infer a requirement of possession would be to add a requirement not expressed by the Legislature." Id. The term "dissemination" also connotes some form of distributive act beyond showing something to another. Id. Consider Commonwealth v. McDonagh, 480 Mass. 131 (2018), where the defendant showed nude pictures on his computer to his minor son. The Commonwealth charged the defendant with various offenses, including dissemination of obscene matter (in violation of Mass. Gen. Laws ch. 272, § 29). Id. at 132. On appeal, the Commonwealth conceded that the evidence was insufficient to prove "dissemination." Id. at 144–45.

2. Computer "Depictions"

"The Legislature was unconcerned with how the photographically created image is stored or communicated." Commonwealth v. Hall, 80 Mass. App. Ct. 317, 326 (2011). "[T]he Legislature's creation of a separate and distinct category for 'depiction by computer' manifests an intent to give special treatment to the unique issues presented by computers, including the fact that stored data, although intangible in their unprocessed form, are readily transferrable to a graphic image." Id. at 327 (quoting Mass. Gen. Laws ch. 272, § 29C).

"Depiction by computer," as that phrase is used in § 29C, includes an unopened file on a hard drive—not only a file that is reduced to a hard copy, or one that is disseminated. Commonwealth v. Hinds, 437 Mass. 54, 63–64 (2002).

3. Child Enticement

"[I]n order to constitute enticement of a victim, the defendant need not physically meet the victim at the same place to which he entices the victim to go" given modern and electronic digital technology. Commonwealth v. Hall, 80 Mass. App. Ct. 317, 323 (2011). In Hall, the Appeals Court noted that the defendant's enticement of the victim via cell phone text messages to go to a private place and take naked photographs to send to him can qualify as enticement. Id. However, given the potentially duplicative offense of posing a child in a state of nudity, the court held that the defendant must lure the child to a place of his/her choosing, not the victim's choosing. Id at 324–25. As this element was missing in Hall, the defendant's enticement charge was set aside. Id. at 325.

4. "Visual Material"

"The Legislature's objective of including a broad range of 'visual material' in its proscription is further demonstrated by Section 31's second sentence which provides: '[u]ndeveloped photographs, pictures . . . and similar visual representations or reproductions may be visual materials notwithstanding that processing, development or similar acts may be required to make the contents thereof apparent.' Thus, in determining whether an image is a 'visual material' within Mass. Gen. Laws ch. 272, the manner of its dissemination is insignificant. Whether further acts are required to make the image apparent to the naked eye, by, for example, keying a computer board, does not render the image any less a 'visual material.'" Commonwealth v. Gousie, 13 Mass. L. Rptr. 585, at *3 (Mass. Super. Ct. 2001) (quoting Mass. Gen. Laws ch. 272, § 29C).

5. "Nudity" Under Mass. Gen. Laws ch. 272, § 31

The SJC examined the definition of "nudity" under §31 in Commonwealth v. Provost, 418 Mass. 416 (1994). In this case, the defendant took photographs of children in the pool and boys in the locker room. Id. at 417–18. One child struck different poses and his partially covered scrotal area was visible in two photographs. Several others showed the child displaying his bare buttocks ("mooning" the defendant). Id. at 418. The SJC provided the following analysis of the statutory meaning of "nudity": "The defendant claims that his activities do not fall within the ambit of § 29A(a). He first contends that the photographs do not depict a minor in a state of nudity within the meaning of, which defines 'nudity' as: 'uncovered or less than opaquely covered human genitals, pubic areas, . . . or the covered male genitals in a discernibly turgid state.' Although [the child] had his underwear on, in two of the photographs portions of his pubic and genital area are clearly visible. The statute does not require that the areas be completely uncovered. It is enough that a portion of the genital area is visible." Id. at 418 (quoting Mass. Gen. Laws ch. 272, § 31).

6. "Performance" Under Mass. Gen. Laws ch. 272. § 29A

A "performance" under Mass. Gen. Laws ch. 272, § 29A "does not expressly or implicitly require the physical presence of 'one or more persons.' In view of the advances in technology, a violation of the statute may occur without the defendant's physical presence." Commonwealth. v. Bundy, 465 Mass. 538, 545 (2013) (finding the statutory definition of performance satisfied by victim masturbating facing a

camera attached to a device that, through an Internet connection, resulted in the image being broadcast to the defendant for him to view).

A "performance" occurs "before one or more persons" even when the only audience member is the person who enticed or encouraged the performance because to hold otherwise would circumvent the plain meaning of "one." Id. at 544.

7. "Knowingly Permit" Under Mass. Gen. Laws ch. 272, § 29A

Mass. Gen. Laws ch. 272, § 29A(b), provides in relevant part: "Whoever . . . hires, coerces, solicits or entices, employs, procures, uses, causes, encourages, or knowingly permits such child to participate or engage in any act that depicts, describes, or represents sexual conduct for the purpose of representation or reproduction in any visual material, or to engage in any live performance involving sexual conduct, shall be punished . . . ." (quoted in Com. v. Bundy, 465 Mass. 538, 539 n.2 (2013)). In Bundy, the jury was instructed as follows on a charge under this statute:

> [I]n proving [the element of live performance], the Commonwealth must establish beyond a reasonable doubt that it was [the defendant's] specific intent to solicit, entice, cause, or encourage [the victim] to engage in a live performance involving sexual conduct. In determining whether the defendant possessed such a specific intent, [the jury] may consider all facts and circumstances, including the defendant's acts and statements. The statute also permits the Commonwealth to establish alternatively that the defendant knowingly permitted [the victim] to engage in a live performance involving sexual conduct.

Id. at 542.

The meaning of "knowingly permit" was at issue in Commonwealth. v. Provost, 418 Mass 416 (1994). The defendant in Provost asserted that "the depiction of [a victim's] pubic area was unintentional and that, since [the victim] voluntarily struck the various poses without instruction, [defendant] did not 'knowingly permit' him to pose in a state of nudity." Id. at 419. The court rejected this argument and held that:

> The photographs themselves suggest that the defendant knowingly permitted [the victim] to pose with a portion of his pubic region and genitals exposed. He took a series of well-focused photographs at various points in the process of [the victim's] dressing. [The victim's] genital area is prominent in many of the photographs. The defendant admitted that he sometimes took photographs of nude boys for sexual gratification. There was sufficient evidence, therefore, for the judge to conclude that the defendant knowingly permitted [the victim] to pose in a state of nudity. Furthermore, the fact that the defendant continued to take the photographs as [the victim] struck different poses certainly supports the inference that he "encouraged" [the victim] to pose in a state of nudity.

Id. at 419.

8. Lewdness

In Commonwealth v. Rex, 469 Mass. 36 (2014), during a standard cell inspection prisoner Rex was found in possession of seven photographs of naked children. Id. at 37. The photos were from National Geographic, a sociology textbook, and a naturist catalogue. Id. The Court held that the indictment for possession of child pornography was properly dismissed because the children depicted were not in unnatural poses and their genitals were not the focus of the photo. Id. at 47. Thus the photos did not depict lewdness—just nakedness. Id. at 47–48. "It is well settled that nudity alone is not enough to render a photograph lewd." Id. at 44 (quotation omitted).

C. Special Conditions of Probation

Special conditions of probation can be unconstitutionally vague — facially or as applied — if they do not give fair notice to a defendant of the scope of prohibited activity. Commonwealth v. Ruiz, 453 Mass. 474, 479 (2009). A defendant "cannot be found in violation of probationary conditions that might have been intended or would have made sense, only of those that are unambiguous and of which he has notice," Commonwealth v. King, 96 Mass. App. Ct. 703, 710(2019) (citing Commonwealth v. Lally, 55 Mass. App. Ct. 601, 603 (2002)), and "ambiguities in probation conditions are construed in favor of the defendant." Lally, 55 Mass. App. Ct. at 603 (citing Commonwealth v. Power, 420 Mass. 410, 421 (1995)).

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography." Id., at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. The court found this sufficed to put the defendant on fair notice that possession of "explicit stories describing the rapes of young children" would violate his probation. Id. at 786-87. However, the court found that a reasonable person would not consider photographs of adults in their underwear or with their hands covering their genitals to be pornographic. Id. Therefore, they were not "so inarguably pornographic as to put the defendant on fair notice that he was violating probation by possessing them," where the photographs "depicted no sexual activity or nudity, and it [was] unclear whether the intent behind them was to arouse sexual excitement." Id. at 786.

  Commonwealth v. King, 96 Mass. App. Ct. 703 (2019). Defendant, who had pled guilty to possession of child pornography, was subject to special probation conditions which provided, in relevant part, that: "(3) The probationer shall not access any internet services from any handheld device (e.g., Palm Pilots, Blackberries, and mobile telephones)"; and "(4) The probationer shall not use, enter, visit, participate in, or remain in any online chat room, bulletin board service, message board service, social networking site or service (for example, Facebook.com, Twitter.com, Instagram.com), or any other online communication service, with the sole exception of electronic mail." Id. at 704. The discussion during the plea colloquy clarified the scope of these two conditions such that, in summary, the third condition prohibited any Internet access from

handheld devices, and the fourth condition prohibited the use of social media on any device (except email). Id. at 705. When read together, the two conditions appeared to permit non-social-media Internet access (including email) from non-handheld devices. Id. While on probation, the defendant accessed "images of young girls wearing scanty dance costumes in provocative poses" and annotated print-outs of these materials by hand with the girls' names, ages, information about their siblings, and smiley faces in some cases. Id. at 706. He accessed these and similar materials using search engines (e.g., Google) and Wikipedia on computers, and emailed some of them to himself. Id. at 705. While acknowledging that the defendant's conduct was "troubling," the appeals court held that "the evidence was insufficient to permit the judge to find that he violated special condition four," because "[s]pecial condition four did not prohibit the defendant from using the Internet generally, or downloading information from it." Id. at 710 ("the defendant cannot be found in violation of probationary conditions that might have been intended or would have made sense, only those that are unambiguous and of which he has notice.").

In dicta, the King court wrote: "with the benefit of appellate hindsight, one cannot help but ask whether special condition four should not have been written differently and, in particular, whether it should have expressly prohibited the defendant from using a computer to access images or information about children, whether via the Internet or otherwise." Id. at 710. Further, "recogniz[ing] both the importance and difficulty of drafting clear special conditions of probation, especially when they involve technology," the court suggested it would "be helpful to supplement existing sources with a set of model, nonbinding special conditions" "for sex offenders and those who use technology to commit crimes," among others. Id. at 711.

Special conditions of probation that refer to pornography may use the "common meaning" of pornography, and may prohibit constitutionally protected activity that may not be the basis of an independent criminal conviction. Hamilton, 95 Mass. App. Ct. at 787.

- Commonwealth v. Hamilton, 95 Mass. App. Ct. 782 (2019). Defendant pled guilty to possessing child pornography and failing to register as a sex offender, and a judge placed a special condition on the defendant's probation that he "not possess pornography,." Id. at 783. The judge defined pornography as "pictures or writings of sexual activity intended solely to excite lascivious feelings of a particularly blatant and aberrant kind." Id. Defendant argued that under Free Speech Coalition, which held facially unconstitutional a statute that criminalized possession of "sexually explicit images that appear[ed] to depict minors" but were actually "created by using adults who look like minors or by using computer imaging," Ashcroft v. Free Speech Coalition, 535 U.S. 234, 239–40 (2002), the explicit stories he posessed were not pornography because they were "'fantas[ies]' that [did] not involve actual children." Hamilton, 95 Mass. App. Ct. at 787. The court rejected defendant's argument, noting "that a probation condition is enforceable, even if it infringes on a defendant's ability to exercise constitutionally protected rights, so long as the condition is 'reasonably related' to the goals of sentencing and probation." Id. (quoting Commonwealth v. Lapointe, 435 Mass. 455, 459 (2001)). The court was not considering a facial challenge to a criminal statute, but rather had to decide the question of "whether a reasonable person in the defendant's circumstances would have known that the stories constitute

pornography in violation of his probation conditions." Id. Thus, "[t]he discussion in Free Speech Coalition [was] not germane to that question because the common meaning of pornography is not limited to materials depicting actual people. For example, had the defendant been found in possession of computer-generated images of what appeared to be children engaging in sexual activity, he indisputably would have been in violation of his probation, even though Free Speech Coalition says that those same images cannot be the basis of a criminal conviction." Hamilton, 95 Mass. App. Ct. at 787.

IV. Expert Testimony About Technology

Expert testimony is ordinarily required when the subject of the testimony "is beyond the common knowledge or understanding of the lay juror." Commonwealth v. Sands, 424 Mass. 184, 186 (1997). Even if a juror does not have personal experience of a technology, a lay juror, from common experience and knowledge, may understand the required concepts when provided sufficient non-expert testimony and evidence. Commonwealth v. Bundy, 465 Mass. 538, 546 (2013) (finding the victim's testimony and photographic evidence sufficient to keep jurors from engaging in conjecture about an Xbox and its accessories) (citing Commonwealth v. Sands, 424 Mass. 184, 186 (1997)).

- Commonwealth v. Javier, 481 Mass. 268 (2019). In this first-degree murder case, the defendant argued, among other things, that the trial judge erred in admitting opinion testimony by a cell phone company employee interpreting CSLI information. Id. at 269. The defendant argued that the employee, who was not an engineer, should not have been permitted to testify about how cell sites operate and how to locate a cell phone based on historical cell site information. Id. at 277, 285. The SJC noted that it had previously expressed some doubt—in an appeal by the defendant's co-venturer, see Commonwealth v. Gonzalez, 475 Mass. 396 (2016)—about the propriety of the phone employee's testimony in two respects. Javier, 481 Mass. at 286. In particular, the SJC explained in Gonzalez that the employee's testimony "'that calls are 'typically' transmitted through the closest cellular site, and that a call from [a particular] address was unlikely to have been transmitted through [a particular cell site] . . . may well have required a witness with greater technical expertise.'" Id. (quoting Gonzalez, 475 Mass. at 412 n.37). The Javier Court also noted, however, that the employee "properly qualified his testimony and explained that, even where a particular cellular telephone was most likely to connect to the nearest tower, there were many reasons why that might not happen," and therefore "the fact that he did not know or investigate the reasons why particular calls had connected to particular towers did not prejudice the defendant." Id. at 286. The SJC concluded that, "while it might have been better practice to exclude evidence that was of little assistance to the jury and that possibly could have been confusing, the judge did not abuse her discretion in allowing [the phone employee's] testimony about certain aspects of the CSLI." Id. at 286–87. Moreover, the portion of the employee's testimony "concerning the reasons that cellular telephones connect to cell towers, and what he 'expected' a particular telephone would be most likely to do here, would not have had any impact on the jury's verdict." Id. at 287.

- Commonwealth v. Moore, 90 Mass. App. Ct. 1106, at *3 (2016) (unpublished). In an appeal from convictions for possession and dissemination of child pornography claiming ineffectiveness of counsel for failure to object to the testimony of the Commonwealth's digital evidence analyst and to request a Daubert-Lanigan hearing to challenge the reliability and the admissibility of his testimony, the Appeals Court found the claim unfounded. Id. at *3. The prosecution's case was based on evidence found on the defendant's laptop. Id. at *1. The AGO analyst connected the laptop's hard drive to a "write blocker"—thus preventing any data additions or removals—and then created a duplicate image of the drive with a program called Encase. Id. A search of the duplicate image resulted in the discovery of three (3) peer-to-peer file sharing programs: "(1) LimeWire (containing more than 900 videos and images of child pornography); (2) eMule (containing more than 400 videos of child pornography); and (3) Ares (containing several search terms consistent with child pornography)." Id. at *1 The AGO analyst also examined the browsing history, text messages, and photographs on the laptop and the defendant's cell phone to corroborate his ownership and exclusive use of the two items. Id. The court found that the Commonwealth presented a strong case at trial and that "the defendant [did] little more than offer [u]nsupported speculation that further examination of the reliability and the admissibility of the prosecution's expert testimony would have undermined the prosecution's case." Id. at *3 (quotation and citation omitted).

V. List of Cases Organized by Device/Evidence Type

This section provides a quick reference list of the cases that appear elsewhere in this Guide, organized by device or evidence type. Case descriptions are in the respective sections where they are discussed.

A. Cell Phone Searches

- Riley v. California, 134 S. Ct. 2473 (2014).
- Commonwealth v. Barillas, 484 Mass. 250 (2020).
- Commonwealth v. Barrett, 97 Mass. App. Ct. 437 (2020).
- Commonwealth v. Fencher, 95 Mass. App. Ct. 618 (2019)

B. Search of Computer Files

- Commonwealth v. Ericson, 85 Mass. App. Ct. 326 (2014).
- Commonwealth v. McDermott, 448 Mass. 750 (2007).
- Commonwealth v. Kaupp, 453 Mass. 102 (2009).
- Commonwealth v. Gousie, 13 Mass. L. Rptr. 585 (Mass. Super. Ct. Sept. 26, 2001) (unpublished).

C. Email

- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

D. CSLI, GPS, and Other Location Technologies

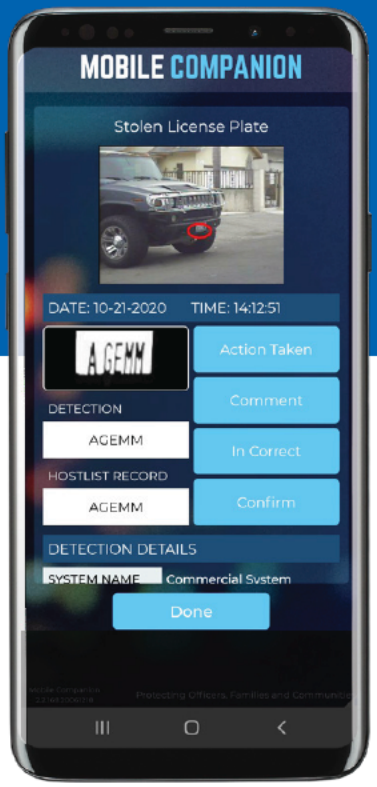
- Carpenter v. United States, 138 S. Ct. 2206 (2018).
- United States v. Jones, 565 U.S. 400 (2012).
- Commonwealth v. Gosselin, 486 Mass. 256 (2020).
- Commonwealth v. Wilson, 486 Mass. 328 (2020)
- Commonwealth v. Davis, 97 Mass. App. Ct. 633 (2020).
- Commonwealth v. Wilkerson, 486 Mass. 159 (2020).
- Commonwealth v. McCarthy, 484 Mass. 493 (2020).
- Commonwealth v. Mora, 485 Mass. 360 (2020).
- Commonwealth v. McMann, 97 Mass. App. Ct. 558 (2020).
- Commonwealth v. Watkins, 98 Mass. App. Ct. 419 (2020).
- Commonwealth v. Vasquez, 482 Mass. 850 (2019).
- Commonwealth v. Hobbs, 482 Mass. 538 (2019).
- Commonwealth v. Fredericq, 482 Mass. 70 (2019).
- Commonwealth v. Lugo, 482 Mass. 94 (2019).
- Commonwealth v. Almonor, 482 Mass. 35 (2019).
- Commonwealth v. Feliz, 481 Mass. 689 (2019).
- Commonwealth v. Johnson, 481 Mass. 710 (2019).
- Commonwealth v. Raspberry, 93 Mass. App. Ct. 633 (2018).
- Commonwealth v. Johnson, 91 Mass. App. Ct. 296 (2017).
- Commonwealth v. Balboni, 89 Mass. App. Ct. 651 (2016).
- Commonwealth v. Estabrook, 472 Mass. 852 (2015).
- Commonwealth v. Augustine, 467 Mass. 230 (2014).
- Commonwealth v. Collins, 470 Mass. 255 (2014).

E. Text Messages

- R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020) (Cypher, J.).
- Commonwealth v. Fulgiam, 477 Mass. 20 (2017).

VIGILANT MOBILE COMPANION

INTELLIGENCE IN THE PALM OF YOUR HAND



Cameras are not always in the right place at the right time, causing you to miss collecting valuable data. Vigilant Mobile Companion transforms your mobile device into a powerful, secure license plate recognition (LPR) and facial recognition data collection, analysis and alerting tool – increasing productivity and insight, anywhere you go.

KEY BENEFITS

Canvas and Collect More Vehicle Data

When it comes to data, too much is never enough. Vigilant Mobile Companion takes what were once manual processes and speeds them up with this simple to use application. Quickly scan a single plate or use multi-plate mode to easily capture plates at scale. Also upload additional images of a vehicle directly to an LPR record for future reference.

Immediately Identify Vehicles of Interest

When security and safety are on the line, every second counts. With Vigilant Mobile Companion receive real-time alerts when hot listed plates are scanned with your device or by selected LPR cameras. Conduct further analysis by viewing historical LPR alerts or by accessing Vigilant LEARN or Vigilant ClientPortal mobile for a full suite of capabilities.

Positively ID Suspects and Victims Faster

The faster you know who the faster a case can be resolved. Vigilant Mobile Companion provides the ability for you to more quickly identify persons of interest, right on scene. Capture a facial image of a person in the field, scan the barcode on a state ID and send data directly to the Vigilant FaceSearch gallery for confirmation or further investigation.

Always Stay Informed and In Control

Having quick and easy access to your data is a game changer – but not if it sacrifices security. Vigilant Mobile Companion is available for both Android and iOS devices with strict access permissions and control set by your agency. Users can rely on either cellular or wifi connectivity for data upload but also have peace of mind knowing that the data is erased when you close the app.

MOTOROLA SOLUTIONS



PRIMARY FEATURES

Simple Plate Image Capture – Quickly and easily scan a single plate with your device for immediate investigative use.

Multi-Plate Scanning Mode – Capture plates at scale of vehicles with multi-plate mode, saving time and manpower.

Manual Plate Image Upload – Manually upload an image of a single plate for future reference.

Vehicle Image Upload – Quickly capture and upload additional images of a vehicle directly to an LPR record for future reference.

In-App & Push Notification Alerts – Receive real-time alerts when hot listed plates are scanned with your device or by selected LPR cameras.

Parking Zone Auto-Selection – Assign scanned plates to a predefined location for easier access and investigation.

Review Historical Alerts – Display historical LPR alerts within a specific location during a set period of time with the alert event function.

Vigilant LEARN & Vigilant ClientPortal Mobile Access – Easily access the same tools found in Vigilant LEARN and Vigilant ClientPortal for analysis and investigations.

Guided Facial Image Capture – Quickly capture an image of a person in the field and upload to the Vigilant FaceSearch gallery.

Manual Face Image Upload – Easily upload image to a Vigilant FaceSearch gallery for confirmation or further investigation.

Face-Based Record Creation – Create a record that contains additional data points and tie it to an image to enhance your future investigations.

QR & Barcode Data Collection – Scan the barcode on a state ID and assign to an image to be uploaded to the gallery.

Android & iOS Availability – Conveniently access Vigilant Mobile Companion from any Android or iOS device.

Secure Cellular or Wifi Upload – Device data is safe and secure with cellular or wifi upload.

Intelligent Data Protection – Close and erase data protection ensures data is removed from your phone when you exit the app.

Agency Managed Access Control – Alert management and access controls for each user is easily managed by the Agency Manager for security and accountability.

Interested in receiving a demo?
Visit motorolasolutions.com/contactus

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved. 12-2020



REAPERHD MOBILE LPR CAMERA SYSTEM

DEPLOYABLE ON ANY VEHICLE. INTUITIVE FOR ANY DRIVER.

Create added awareness on the road. The ReaperHD Mobile License Plate Recognition (LPR) Camera System is a complete solution that can be deployed on any vehicle in your fleet and easily operated by any driver. It enables your team to receive real-time alerts, conduct comprehensive searches and, paired with Vigilant PlateSearch or Vigilant ClientPortal, leverage advanced analytics and parking tools to uncover new vehicle location insights that protect communities and generate revenue.

KEY BENEFITS

Detect As You Drive
Deploy a purpose-built LPR camera system, configured for your needs and optimized for mobility – to go where you go.

Rely On Better Basics
Beyond ensuring you've captured the best data, we make management, alerting and searching straight-forward.

Do More With More Data
Use patented analytics and access to billions of detections to derive new intelligence and more valuable insights.



MOTOROLA SOLUTIONS

REAPERHD MOBILE LPR CAMERA

High definition, low profile and with various mounting options, our ReaperHD mobile LPR camera can capture nearly 60 scans per second for analysis, even in the most extreme environment.



CAMERA PERFORMANCE

Part Number	Optimal Focal Length	Capture Range
VSR-42-925	75 ft / 22.9 m	55-80 ft / 16.8-24.2 m
VSR-42-916	34 ft / 10.4 m	20-55 ft / 6.1-16.8 m
VSR-42-912	24 ft / 7.3 m	13-48 ft / 4.0-14.6 m
VSR-42-908	16 ft / 4.9 m	8-36 ft / 2.4-11.0 m
VSR-42-906	12 ft / 3.7 m	6-24 ft / 1.8-7.3 m

OPTICS

Window	Shatterproof window
Resolution	1.51 - 2 MP
Capture speed maximum	150 mph (241 kph)

HOUSING

Size	W 6.9 / L 3.9 / H 2 in (W 175 / L 98.5 / H 52 mm)
Fixed mounting	3-axis (aim precision) lock in place, low profile, solid mount, and sun shield
Color	Matte black
Weight	2.2 lbs / 1 kg

ENVIRONMENTAL

Environmental protection	IP67 / NEMA4 compliant
Operational temperature	-40°F to 140°F (-40°C to 65°C)
Connector	IP67 rated RJ45 female

ELECTRICAL

Power consumption	15W nominal, 25W max
Input voltage	POE+ (IEEE802.3 at PD)

CABLE MANAGEMENT

Cable length	Up to 328 ft (100 m)
Type	Cat6 STP 22-24 AWG
Connector	IP67 RJ45 male connector (camera end); RJ45 male (injector end)

VLP PROCESSOR

The VLP Processor combines processing and power in a durable, ruggedized enclosure that is equipped with an all-in-one built-in processor with GPS and PoE for up to four cameras.



SYSTEM	
CPU	Intel Gen8 Core i7-8700T (12M Cache 2.4GHz up to 4.0GHz)
Memory	2 x 8GB DDR4 2400 MHz SO-DIMM
LAN Chipset	9 x Intel i210-AT and 1 x i219 (iAMT9.5 w/ i5, i7 only) Gb/s Ethernet Controllers Onboard Support PXE and WOL

I/O	
Serial Port	3 x RS 232/422/485 (Auto Direction Control)
USB Port	4 x USB 3.0 Ports
LAN	10 x RJ45 Ports for GbE (Optional for M12 connector and 8 x PoE total Max. 120W)
Video Port	3 x DP Ports
Wi-Fi Adapter	802.11n/g/b
4G LTE / GPS	Sierra Wireless EM7511-Dual Sim Support

POWER REQUIREMENT	
Power Input	12V DC
Power Protection	Automatic Recovery - Short Circuit Protection
Power Management	Remote/Ignition connection to toggle power
Power Off Control	Power off Delay Time Setting by BIOS and Software

SOFTWARE	
Operating System	Ubuntu 18.04 64bit

GRAPHICS	
Graphics	Intel® UHD Graphics 630
Resolution	Max Resolution (DP) : 4096x2304@60Hz

STORAGE	
Type	2 x 2.5" Drive Bay for SATA Type HDD/SSD RAID 0, 1, 5 1 x mSATA

ENVIRONMENTAL	
Operating Temp.	-40°C ~ 70°C, ambient w/ 0.6m/s airflow
Storage Temp.	-40°C ~ 80°C
Relative Humidity	10% RH – 90% RH (non-condensing)
Vibration (random)	EC60068-2-64, random, 2.5G@5~500Hz, 1hr/axis with SSD
Vibration Operating	MIL-STD-810G, Method 514.6, Procedure 1, Category 4
Shock	Operating: MIL-STD-810G, Method 516.6, Procedure 1, Trucks and semi-trailers=15G (11ms) with SSD
Certifications	CE, FCC Class A, E13

MECHANICAL	
Construction	Polycarbonate
Mounting	Wall or pole mount
Weight	5190g
Dimensions	260(L) x 250(W) x 95(H) mm

VIGILANT CARDETECTOR MOBILE

Vigilant CarDetector Mobile in-car system software alerts drivers when a license plate on a hot list is scanned, can be used to search plates as well as manage systems.



HARDWARE	MINIMUM REQUIREMENTS	RECOMMENDED REQUIREMENTS
Processor	Intel Core i3-8145U @ 2.10GHz (or 3,847+ PassMark Score)	Intel Core i7-3632QM Processor (6M Cache, up to 3.20 GHz) (or 6,929+ PassMark Score)
Memory	8 GB RAM	16 GB RAM
Hard Drive	256 GB SATA III SSD Drive @ 550 Mbps Read/Write Speed	500 GB M.2 SSD Drive @ 550 Mbps Read/Write Speed or higher

SOFTWARE	MINIMUM REQUIREMENTS	RECOMMENDED REQUIREMENTS
Operating System	MS Win 7 (Professional Version - 64 Bit)	MS Win 10 (Professional Version – 64 bit)

NETWORK	MINIMUM REQUIREMENTS	RECOMMENDED REQUIREMENTS
Ports Utilized	TCP 2000, 3000, 4000, 5000 (LAN /DSP)	TCP 2000, 3000, 4000, 5000 (LAN /DSP)
	TCP Port 3310 (Internal for database)	TCP Port 3310 (Internal for database)
	TCP Port 80, 443, 8888 (Wireless to LEARN)	TCP Port 80, 443, 8888 (Wireless to LEARN)
Network Card	1.0 Gbps	1.0 Gbps
Internet	3G	4G

Please Note: *The above charts reflect MDC configurations for use with the VLP communications box and up to a 4-camera LPR system.*



VLS MOBILE TABLET (OPTIONAL)



The VLS Mobile Tablet is cost efficient, compact and rugged, with a built in processor that supports up to three LPR cameras[1] and GNSS, along with Vigilant CarDetector Mobile without the need for deploying the VLP Communications Box.

SYSTEM	
CPU	Intel® 8th Generation Core™ i7 quad-core processor
RAM	16GB
Storage	256GB
Operating System	Microsoft® Windows® 10 IoT Enterprise
NIST Compliance	NIST compliant BIOS
Display	10.1" LED backlight, high-brightness (800 nits) screen with capacitive multi-touch, outdoor viewable
Display Resolution	1920 x 1200
Network Interface	Wi-Fi 802.11ac, 2.4GHz/ 5GHz dual band; Bluetooth 4.2 LE
Fan/ Fanless	Fanless
Control Switch and Buttons	1 power button, 3 programmable buttons, RF switch
Indicator	1 power/battery status LED
Microphone	Built-in microphone with DSP for real-time video
Speaker	Built-in speaker

I/O PORTS	
USB Port	1 (USB 3.0)
Audio Jack	1 (3.5mm)
DC-in	1
Smart Card/CAC Reader	Full slot, reads ISO 7816 T=0, T=1; 1.8/3/5V smart card

MECHANICAL AND ENVIRONMENTAL	
AC/DC Adapter	Input: 100 – 240V AC; Output: 19V DC, 3.42A
Battery Pack	Hot swappable battery, 11.4V, 5400mAh Hot swappable battery, 11.4V, 8000mAh (optional)
Enclosure	ABS + PC plastics and magnesium-aluminum alloy
Protective Bumpers	Rubber bumpers on each corner for handling protection
Dimensions (H x W x D)	7.8 x 11 x 0.86 in/ 198 x 280 x 21.9 mm
Weight	3.1 lbs/ 1.4 kg
Durability	IP65, MIL-STD-810G and MIL-STD-461F certified
Regulatory	FCC Class B, CE, RoHS compliant
Temperature	Operation*: -20°C to 60°C (-4°F to 140°F); tested under MIL-STD-810G method 501.6, Procedure II, and method 502.6, Procedure II
Storage*	-55°C to 70°C (-67°F to 158°F)
Humidity	0% – 90% non-condensing

**For battery safety and optimal functionality and performance, the recommended usage temperature range is from -10°C to 45°C (14°F to 113°F)*

MAJOR OPTIONS SPECS	
Barcode Scanner	2D barcode scanner; reads 1D also
Camera	8 megapixel back camera with auto focus, white balance, gain control and exposure control
GNSS Module	U-blox M8 GNSS module with concurrent reception of GPS and GLONASS, industry leading -167dBm navigation sensitivity
Mobile Broadband	4G module for LTE, HSPA+, GSM/GPRS/EDGE, EV-DO, Rev A and 1xRTT

1. Three cameras only for low speed, low volume operation, two cameras are recommended for higher speed, higher volume environments. Please consult with your Motorola Solutions representative to determine what will work best for you.

SYSTEM ACCESSORIES

VEHICLE BRACKETS

Vehicle Make/Model	Vehicle Year	Roof Mount – Part #	Trunk Mount – Part #	Hood Mount – Part #
Chevrolet Tahoe	2006-14	K-U-R-TAHOE-06-SET		
Chevrolet Tahoe	2015+	K-U-R-TAHOE-SET	K-U-T-CAP-SET	
Chevrolet Caprice	ALL	K-U-R-CAP-SET		
Dodge Charger	2011+	K-U-R-CHGR11-SET	K-U-T-CHGR11-SET	
Dodge Charger	2005-2010	K-U-R-CHGR-05-10-SET	K-U-T-CHGR-05-10-SET	
Ford Crown Victoria	ALL	K-U-R-CVIC-SET	K-U-T-CVIC-SET	K-U-H-CVIC-SET
Ford F-150	2014+	K-U-R-F150-14-SET		
Ford Transit	2016+	K-U-R-TRANS-SET		
Ford Escape	ALL	K-U-R-ESC-18-SET		
Ford Interceptor – Sedan	ALL	K-U-R-INTSDN-SET	K-U-T-INTSDN-SET	
Ford Interceptor – SUV	2013-2019	K-U-R-INTSUV-SET		
Ford Interceptor – SUV	2020+	K-U-R-INTSUV-20-SET		

LIGHTBAR BRACKETS

Lightbar Mfg or Universal	Style	Lightbar Mount – Part #
Federal Signal	Valor-Complete Set	VS-LBB-FS-VBAR-02-A
Federal Signal	Valor w/ TD Relocation Kit-Complete Set	VSS-LBB-FS-VBAR-02-DKIT
Universal	Single Bracket- Compatible w/ most Whelen/Code3	VS-LBB-01-E
Universal	Complete Set- Compatible w/ most Whelen, Code3, TOMAR, Federal Signal, Arjent S2	VS-LBB-02-E

UNIVERSAL MOUNTS

Style	Universal Mount – Part #
Magnet Mount	U-BASE-SET
Push Bumper	K-PB-HD-SET
Ram Ball Set (Trailers and Covert)	CAM-HITCH-SET
Universal Camera Bracket	CAM-MOUNT-FLAT-ASSY-SET

For more information,
visit motorolasolutions.com/contactus

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved. 02-2021

Massachusetts Department of State Police
Automated License Plate Recognition (ALPR) System
Memorandum of Understanding and Agreement

THIS AGREEMENT, made and entered into this _____ day of _____, 2022 by and between the Department of State Police, hereinafter referred to as "Department," and the

_____,

a public entity, hereinafter referred to as "Agency," collectively referred to as "Parties."

WHEREAS, the Department contracts the services of one or more vendors to host an Automated License Plate Recognition (ALPR) database to store ALPR data; and

WHEREAS, the Parties provide Public Safety services within their respective jurisdictions; and

WHEREAS, the Parties have found it to be of mutual benefit to provide for the most efficient utilization of their resources and services in the application to Public Safety efforts within their respective jurisdictions; and

WHEREAS, the Parties are committed to cooperation and coordination in providing the highest level of public safety services to the public, guided by the principle that performing cooperatively is in the best interest of the public; and

WHEREAS, the Agency desires to use the ALPR system contracted and managed by the Department to facilitate the storage of ALPR information generated by the Agency; and

WHEREAS, the Agency desires to share law enforcement information owned by the Agency under the conditions set forth in this Agreement; and

WHEREAS, it is the mission of the Parties to locate and assist citizens who may be lost, missing, kidnapped, ill, or endangered, as it is the mission of the Parties to protect citizens from the threat of violent crime, narcotics trafficking, and international and domestic terrorism related activities through information sharing and technical operation support to public safety agencies.

NOW, THEREFORE, for and in consideration of the covenants contained herein, IT IS HEREBY AGREED, by and between the Parties as follows:

1. PURPOSE:

The purpose of this Agreement is to provide a standardized approach and method of storage, sharing, and access of ALPR data between the Department and Public Safety Agencies hosting ALPR cameras on the Department's ALPR system.

2. COSTS:

The Department shall be responsible for the costs of purchasing and maintaining the ALPR system as long as such funding is available to the Department and authorized by the appropriate authorities of the Commonwealth. Participating agencies shall be responsible for the costs of purchasing, servicing, maintaining, repairing, and/or licensing the ALPR equipment used by their respective agency. The Department shall not be responsible for any costs incurred by the Agency for the purchasing, servicing, maintaining, repairing, and/or licensing of the ALPR equipment owned or used by the Agency.

3. DATA ACCESS AND SECURITY REQUIREMENTS:

a. System Availability: The Department will work with the vendor(s) to keep the ALPR system software and servers online and available with downtime limited to necessary system maintenance activities or to any outages that are beyond the control of the Department.

b. Data Sharing: ALPR data contributed by the Agency will be accessible for official purposes to all Agencies that have entered into an ALPR Agreement with the Department. The Agency shall not otherwise share ALPR data with or provide ALPR data to any person, entity, or government agency, other than a law enforcement agency, unless such disclosure is authorized by policy or court order or unless such disclosure is required by the Massachusetts Rules of Criminal Procedure or Rules of Superior Court governing discovery in criminal matters.

c. Security Requirements: The Department and the Agency agree to enforce and maintain security requirements for the information stored in the ALPR system as specified in the Agreement. Agency agrees that the information hosted in the ALPR system shall be used for law enforcement purposes only and that only law enforcement agency employees that have been subject to background screening will be allowed access to the system.

   Background screenings must be fingerprint-based and include check of both the state and national criminal history repositories. If a felony conviction of any kind is found,

access to ALPR system shall not be granted. Agency agrees not to share passwords, user logins, or allow the ALPR software to be otherwise used by agencies who have not entered into an Agreement with the Department allowing such activity.

An employee of the Agency may operate an ALPR unit that is connected to the ALPR system or access the ALPR system software only if the person is a sworn law enforcement officer, has been designated as an authorized user by the Chief of the Agency or designee, and has received training from the Agency or the Department on the proper use and operation of ALPRs and any policy or procedures governing the use of ALPRs and ALPR data issued or adopted by the Agency.

4. IMPLEMENTATION OF POLICY:

The Agency shall, within 30 days of execution of this Agreement, if not already in existence, promulgate and enforce a rule, regulation, standard operating procedure, directive, or order, in a form as may be appropriate given the customs and practices of the agency, which shall regulate the Agency's use of and interaction with the ALPR system, and which shall provide that any sworn officer or civilian employee of the Agency who knowingly violates the Agency's rule, regulation, standard operating procedure, directive, or order shall be subject to discipline.

In the alternative, the Agency may elect to adopt the Department's General Order TRF-11 as the policy and procedure document that will govern the Agency's use of and interaction with the ALPR system. In this event, the Agency agrees that it has been provided with physical or electronic copy of General Order TRF-11, has had sufficient time to read, review, and understand the document in its entirety, and agrees to be bound by the provisions contained therein. In this event, the Department agrees to inform the Agency of an updates or modifications to General Order TRF-1, and the Agency understands and agrees that any updates to General Order TRF-11 will be binding upon the Agency unless the Agency elects to terminate the Agreement and withdraw from participation in the ALPR system.

5. BENEFITS TO AGENCY:

a. Data Links: The centralized storage of ALPR data will provide a solution to the problem of inaccessible or irretrievable information as result of disconnected ALPR systems and the difficulty in sharing information across jurisdictional boundaries.

b. Reduction of Costs: The centralized storage of ALPR data will reduce the financial burden to the Agency that is associated with purchasing and maintaining ALPR software.

6. RECORDS AND REPORTS:

The Department protects all ALPR information as personally identifiable information (PII) because ALPR information may be combined with other information to specifically identify a unique individual. However, information stored in the ALPR system for the Agency may be subject to disclosure under certain circumstances. The Department will refer all public records requests for Agency information to the Agency to respond. However, the Department may be required by law to release the information directly to the requesting party.

7. AMENDMENTS:

Any changes and additions to this Agreement shall be made by written amendments to this Agreement and shall not be effective until approved in writing by the Parties. A joint review of this Agreement may be requested at any time by either of the Parties to identify needed changes, which may be amended by written mutual agreement of the Parties.

8. DURABILITY:

This Agreement shall become operational and effective upon execution by the Parties. Parties may terminate the Agreement at any time by giving written notice to the other Parties at least thirty (30) days prior to the effective date of termination. The Agreement may also be terminated by the Department without prior notice to the Agency in the event of executive, legislative, or judicial mandate which requires the unanticipated discontinuation or modification of the ALPR program. In the event of such termination, the Department will notify the Agency as soon as practicable.

9. BENEFITS:

The Parties shall agree that the provisions of this Agreement are not intended to directly benefit and shall not be enforceable by any person or entity not a party to this Agreement. This Agreement is not intended to confer any legal rights or benefits on any person or entity other than the Parties of this Agreement.

10. INDEMNIFICATIONS:

Parties shall defend, indemnify, and hold harmless every other party and its officers, agents, employees, and representatives from any and all losses, liability, damages, claims, suits, actions and administrative proceedings, and demands and all expenditures and cost relating to acts or omissions of the indemnitor, its officers, agents, or employees arising out of or incidental to the performance of any of the provisions of this Agreement. Parties do not assume liability for the

acts or omissions of persons other than their respective officers, its employees, agents, and MOU officers.

The Agency releases the Department from any liability relating to the loss or destruction of data contributed by the Agency. The Agency further releases the Department from any liability relating to the loss of the Agency's access to the ALPR system due to system outage, commercial vendor failure or malfeasance, or executive, legislative, or judicial mandate which requires the unanticipated discontinuation or modification of the ALPR program. The Agency further releases the Department from any liability relating to the release of data or information contributed by the Agency pursuant to a lawful procedure or order.

11. ASSIGNMENT PROHIBITED:

Parties to this Agreement may not assign any right or obligation pursuant to this Agreement. Any attempted or purported assignment of any right or obligation pursuant to this Agreement shall be void and of no effect.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the date as written below.

_____	_____
	Representative:
Massachusetts State Police	Agency:
_____	_____
Date	Date

Memorandum of Understanding
South Bay Information Sharing System (SBISS)
SOUTH BAY REGION NODE

This Memorandum of Understanding ("MOU") is made and entered into on this ___ day of _____ and year _____ by and between the parties below and all future signers of this Agreement, known collectively as "Member Agencies" or individually as a "Member Agency."

The following Member Agencies hereby create the South Bay Information Sharing System (SBISS) SOUTH BAY REGION NODE (Node): The following agencies are collectively known as the "Original Member Agencies."

Santa Clara County:

- Campbell Police Department
- Gilroy Police Department
- Los Altos Police Department
- Los Gatos-Monte Sereno Police Department
- Milpitas Police Department
- Morgan Hill Police Department
- Mountain View Police Department
- Palo Alto Police Department
- San Jose Police Department
- Santa Clara County Sheriff's Office
- Santa Clara Police Department
- Sunnyvale Department of Public Safety

Santa Cruz County:

- Capitola Police Department
- Santa Cruz Police Department
- Santa Cruz County Sheriff's Office
- Watsonville Police Department

Monterey County:

- Carmel Police Department
- Del Rey Oaks Police Department
- Gonzales Police Department
- Greenfield Police Department
- King City Police Department
- Marina Police Department
- Monterey Police Department
- Monterey County Sheriff's Office
- Pacific Grove Police Department
- Salinas Police Department
- Sand City Police Department
- Seaside Police Department
- Soledad Police Department

San Benito County:

- Hollister Police Department
- San Benito County Sheriff's Office

Additionally, the following Member Agencies hereby also compose the South Bay Information Sharing System (SBISS) SOUTH BAY REGION NODE (Node): The following agencies are collectively known as the “District Attorney Member Agencies.”

- Santa Clara County District Attorney’s Office
- Santa Cruz County District Attorney’s Office
- Monterey County District Attorney’s Office
- San Benito County District Attorney’s Office

Additionally, the following Member Agencies hereby also compose the South Bay Information Sharing System (SBISS) SOUTH BAY REGION NODE (Node): The following agencies are collectively known as the “University Police Member Agencies.”

- California State University, Monterey Bay Police Department
- San Jose State University Police Department

Additionally, the following Member Agencies hereby also compose the South Bay Information Sharing System (SBISS) SOUTH BAY REGION NODE (Node): The following agencies are collectively known as the “Probation Member Agencies.”

- Santa Clara County Probation Department
- San Benito Probation Department
- Monterey County Probation Department
- Santa Cruz County Probation Department

Purpose

This regional law enforcement information-sharing system shall be known as the SBISS South Bay Region Node. The purpose of this agreement is to maintain the South Bay Region Node, to outline the duties and responsibilities of each Member Agency, to define the working relationships and lines of authority for Member Agencies in the SBISS South Bay Region Node, and to provide for the addition of other eligible entities in the data-sharing program created by this MOU. Member Agencies shall work cooperatively to establish an integrated system of information technology that maximizes the sharing of data and communication between the Member Agencies while maintaining the confidentiality of privileged or otherwise protected information shared through the system. The Member Agencies shall work cooperatively in a variety of ways to facilitate sharing data in an effort to improve the information sharing efforts of their respective Agency and Node.

Santa Clara County Police Chiefs and Sheriff, through a grant from the Office of Homeland Security, have identified the Cities, Counties, and other Agencies within Santa Clara, Santa Cruz, Monterey, and San Benito Counties, including any departments or divisions of such agencies that should enter into this agreement to share data among such agencies.

THEREFORE, the Member Agencies hereby agree to the following:

1 Definitions:

1.1 *South Bay Information Sharing System*: "SBISS" shall mean the collective group of law enforcement and justice agencies, within Santa Clara, Santa Cruz, Monterey, and San Benito Counties who are signatories on a regional law enforcement information-sharing agreement.

1.2 *South Bay Region Node:* "Node" shall mean the collective informational infrastructure of the data warehouse operated for the benefit of the Member Agencies, within the central region of SBISS bound by the terms of this Agreement.

1.3 *South Bay Region Node Board of Directors:* "Board" shall mean the Board of Directors that is the governing body of the South Bay Information Sharing System.

1.4 *COPLINK*: shall mean the information sharing and analysis software licensed to the Fiscal Agent on behalf of the Member Agencies by IBM under the name COPLINK.

1.5 *Criminal Justice Practitioners:* those personnel from the Member Agencies that have the appropriate clearance and authority to utilize and access the Data as a function of their employment, or those agencies that have been approved for read only participation by a majority vote of the Board Members.

1.6 *Data*: shall mean facts, detailed information, or other material provided by a Member Agency.

1.7 *Data Set* is a specific grouping of data included in systems like records management or jail management systems. For example, typical data sets within a records management system include, but are not limited to, Crime Reports, Field Investigations, Citations, Mug shots, and Arrest Reports.

1.8 *Data Records* refers to a unique record associated with an incident or person. For example, this refers to a single report that includes a variety of data.

1.9 *Fiscal Agent*: shall mean the Santa Clara County Office of the Sheriff as approved and directed by the Urban Areas Security Initiative (UASI) to handle and account for funds collected for the benefit of all Member Agencies.

1.10 *Host: shall* mean the Santa Clara County Office of the Sheriff as the entity providing the facilities used to host the Node as determined by the Urban Areas Security Initiative (UASI).

1.11 *International Business Machines*: "IBM" shall mean a corporation with its principal place of business at 1 New Orchard Road, Armonk, New York, 10504-1722, and the owner and developer of the software known as COPLINK.

2 Effective Date and Term of MOU

2.1 Effective Date: The effective date of this MOU is the date noted above and/or the date each subsequent agency executes this Agreement.

2.2 Term: This MOU shall remain in effect and shall be reviewed every three years. The Agreement can only be terminated as provided herein.

3 Board of Directors

3.1 The South Bay Region Node Board of Directors: shall be comprised of eleven (11) Directors and their respective alternates. Alternates shall serve as Directors in the absence of their respective Directors and shall exercise all rights and privileges thereof.

3.1.1 Directors are as follows:

3.1.1.1 One Director shall be the Santa Clara County Sheriff.
3.1.1.2 One Director shall be the Chief of the San Jose Police Department.
3.1.1.3 One Director shall be appointed by the Santa Clara County Police Chief's Association from its membership.
3.1.1.4 One Director shall be the Santa Cruz County Sheriff.
3.1.1.5 One Director shall be the Chief of the Santa Cruz Police Department.

3.1.1.6 One Director shall be appointed by the Santa Cruz County Police Chief's Association from its membership.
3.1.1.7 One Director shall be the Monterey County Sheriff.
3.1.1.8 One Director shall be the Chief of the Salinas Police Department.
3.1.1.9 One Director shall be appointed by the Monterey County Police Chief's Association from its membership.
3.1.1.10 One Director shall be the San Benito County Sheriff.
3.1.1.11 One Director shall be the Chief of the Hollister Police Department.

3.1.2 Each member of the Board shall have one vote. A majority of the members of the entire Board shall constitute a quorum for the transaction of business. Except where a supermajority is required by statute, this MOU or a resolution of the Board, actions by the Board shall require the affirmative vote of a majority of the entire Board (i.e. six (6) affirmative votes).

3.1.3 Every year the Board shall elect a Chair from among its membership to preside at meetings and shall select a Secretary who may, but need not, be one of the eleven Directors.

3.1.4 The Board shall establish and adopt bylaws and a governance process and will set policy for the use of the SBISS South Bay Region Node.

3.1.5 Meetings: The Board shall hold at least one meeting each year, and may schedule additional or special meetings as necessary.

4 Committee and Working Groups

4.1 South Bay Region Node Technology Committee: The Board of Directors may appoint a representative from each Member Agency to serve on the Technology Committee. The Technology Committee Members will serve at the sole discretion of the Board of Directors. The Technology Committee will develop policies relating to data set information sharing. The Technology Committee will meet at least once per year to address system operations, upgrades, enhancements and any other matters of concern to Member Agencies.

4.2 South Bay Region Node Working Groups: The Board is empowered to create, dissolve, or reconstitute working groups, appoint representatives, and perform other actions as deemed necessary to fulfill the purposes

stated herein, including the creation of such groups as an implementation, sustainment or other groups necessary to further law enforcement information sharing efforts.

5 Data Access and Security Requirements

5.1 Data Access: Access to Member Agencies' Data will be provided utilizing a secure network maintained by the Host Node. The Santa Clara County Sheriff's Office will be responsible for the maintenance and care of the secure network. Query capabilities shall be provided to Member Agencies and Authorized Users utilizing any secure network configuration that is acceptable to the Host Node. The information residing in the Data Repositories shall generally be available. Member Agencies agree to inform other Member Agencies in advance, whenever possible, of scheduled down times of specific data feeds. All Member Agencies will be required to sign the COPLINK System Use Agreement and this Memorandum of Understanding prior to gaining access.

5.2 Data Sharing: All Member Agencies agree to share data with other Member Agencies who have a need to know and a right to know, with comprehensive, timely, accurate information about a suspect or offender to include, but not limited to, identity, prior agency contacts, citations, arrests, investigations, criminal history, and current justice status. Each agency will be required to have each employee sign an Employee Statement form agreeing not to misuse the information contained in COPLINK. Each agency will have the prerogative of not sharing those items of data that it deems sensitive or confidential. Nothing in this MOU shall be construed to mean that any Member Agency must share any type of data. The South Bay Region Node Technology Committee will develop a Guideline Document that will make a recommendation for the type of data to be shared by each agency. This document will be a guideline only and will not be binding. The data to be shared, will be the data that the Member Agency already has in its own database and no agency will be required to collect any data that it does not collect in the normal course of business.

The South Bay Region Node Technology Committee will set the criteria for the minimum number of data sets (i.e. Crime Reports, Citations, Field Investigations, Mugs, Arrests Reports, etc.) that member agencies must provide to be a member agency. In addition, the Technology Committee will adopt guidelines for agencies to withhold or suppress certain documents based on specific criteria. Based on these guidelines, each Member Agency shall determine, in the exercise of its sole discretion, which data records are shared within the system. Each member agency

shall maintain their respective source databases. Each Agency shall strive to identify and achieve common interests to enhance public safety and due process while maintaining individual privacy rights.

5.3 Security Requirements: Member Agencies agree to maintain and enforce security requirements for the system. Each Member Agency is responsible for the internal agency security of their records and any technical support necessary to insure proper security. Member Agencies agree to confirm that their network meets current DOJ security requirements as set forth in the most current Policies, Practices and Procedures Document provided by the Department of Justice, and that SBISS will continue to meet those standards.

5.3.1 Liability and Indemnification: Each Member Agency takes legal and financial responsibility for the actions of their employees, officers, agents, representatives and volunteers. Member Agencies agree to indemnify, defend and hold harmless other Member Agencies to the fullest extent permitted by law from and against any and all demands, claims, actions, liabilities, losses, damages, and costs, including reasonable attorney's fees arising out of or resulting from this MOU, and that each agency shall bear the proportionate cost of any damage attributable to the fault of that agency, its governing body, officers, agents, employees and volunteers. It is the intention of the Member Agencies that, where fault is determined to have been contributory, principles of comparative fault will be followed.

5.3.2 Background and Fingerprint Requirements: All persons including non-criminal justice and volunteer personnel who have access to the SBISS South Bay Region Node are required to undergo background and fingerprint check. Each Agency will determine, based on their internal policies and the CLETS Policies, Practices, and Procedures, when SBISS access will not be granted to an employee. The final responsibility for maintaining the security and confidentiality of SBISS information rests with the Member Agency head or administrator.

5.3.3 User Access: Each employee/volunteer is required to sign an employee statement form prior to operating or having SBISS access. Each employee/volunteer shall sign an employee statement on a biennial basis. Additional requirements may be required at the discretion of an agency. A sample form is attached hereto as Exhibit C.

When a person with access to SBISS is no longer employed or no longer accessing SBISS on behalf of the Member Agency, the

Agency is responsible for removing all related passwords and security authorizations from the system.

No person with access to SBISS shall release any information or records located in SBISS without express permission of the Original Agency who provided the data. No person with access to SBISS shall release any information contained in SBISS either by Court Order or in response to a Public Records Act request unless they are the originating agency of such data. All California Public Records Act or Freedom of Information Act requests should be referred back to the originating agency.

5.3.4 Insurance: Each Member Agency, at its sole cost and expense, shall carry insurance or self-insure - its activities in connection with this MOU, and obtain, keep in force and maintain, insurance or equivalent programs of self-insurance, for general liability, workers compensation, and business automobile liability adequate to cover its potential liabilities hereunder. Each Member Agency shall carry a minimum of one million dollars in general liability insurance.

5.4 Connecting with other COPLINK Nodes: The Board will continually work to expand the connectivity of the SBISS South Bay Region Node and will actively pursue opportunities to sign MOU agreements with other COPLINK nodes under the guidelines outlined in this agreement.

5.5 SBISS Node Cooperation: Participating agencies understand that the South Bay Region Node Board of Directors has authorized the Chair of the Board to sign MOU and Inter-Agency agreements with other COPLINK nodes and Law Enforcement Sharing Systems for the purpose of expanding the data sharing network.

6 Information Ownership, Release and Accuracy

6.1 Ownership and Release Constraints: Member Agencies shall retain control of and remain the official custodian of all information they contribute to the South Bay Region Node. All requests for information, California Public Records Act or Freedom of Information Act, will be referred to the Member Agency that is the owner of the requested data, and the Member Agency that is the owner of the requested data will be responsible for responding to the request for information.

6.2 Information Utilization: Any Data present in the COPLINK or law enforcement system is the proprietary information of the Member Agency contributing that Data. Each Member Agency has an affirmative

obligation to assure that any "criminal intelligence data that is entered and used through the COPLINK intel L.E.A.D product complies with 28 CFR Part 23. Member Agencies and Authorized Users may use the Data for Law Enforcement purposes only. The Member Agency responsible for contributing the Data shall have sole discretion regarding release of that information.

6.3 Information Accuracy: Member Agencies and Authorized Users acknowledge that Data maintained in the South Bay Region Node consists of information that may or may not be accurate. Each Member Agency agrees to do an internal audit of their own Data annually in order to review the Data for accuracy. A random sampling of different types of Data shall be selected by each agency to review and compare their Records System Data with the same data in the COPLINK system. Each Member Agency agrees to maintain a copy of their internal audit form for a period of no less than three years for review by the Board of Directors on request. A sample form is attached hereto as Exhibit D and can be used to help facilitate this audit.

6.4 Audit Trail: An Audit Trail will be maintained for a period of no less than three years to determine who accessed the data including the date and time when the data was accessed.

6.5 Data Errors: It will be the responsibility of the Member Agency to correct data errors that have been identified at that Member's sole cost within a reasonable time, but no later than ninety-days (90) from the date of notification.

6.6 Criminal Discovery: Prior to releasing any data in furtherance of its statutory and constitutional obligations relating to the criminal discovery process, a member prosecuting agency shall seek express permission from the originating agency. In order to aid in the release of data, it is recommended that each contributing agency designate a Criminal Discovery Coordinator or equivalent contact person to receive, evaluate and promptly reply to such requests.

In any instance where an originating agency declines to grant such disclosure permission, the originating agency and the prosecuting agency shall confer to reach agreement on possible limitations on disclosure (including the seeking of judicial protective orders) in an attempt to protect the originating agency's specific concerns while allowing the prosecuting agency to meet its statutory and constitutional criminal discovery obligations.

7 Funding, Costs, Personnel and Financial Considerations

7.1 Node Costs: Costs for the creation, initial three (3) years of maintenance and the expansion of the Node was paid for as set forth in the SBISS South Bay Region Node Share of Cost Agreement attached hereto as Exhibit A. Since the initial creation of the node, Exhibit A has and may be amended from time to time and is incorporated herein by reference.

7.2 Payment Administration: The Fiscal Agent shall administer payments to vendors and invoice Member Agencies for their share of cost.

7.3 Financial Responsibility: Initially, the hardware and software required at each Node was paid for with Grant funding. However, in the event grant funding is not available the new Member Agency will be responsible for the expense of acquiring and maintaining the hardware, software, and data communication equipment and services needed by their Agency to connect to the Node. For new member or view-only agencies not part of the cost allocation table all host related support costs shall be allocated to the sustainment of the Node and will not serve as profit. It is understood that as the system ages, there may be certain upgrades or maintenance required on the hardware at each of the Member Agencies. These upgrades or required maintenance will be the sole responsibility of the Member Agencies. Nothing included in this MOU requires any Agency to directly fund the activities of any other Member Agency. Future upgrades to the Servers and Core Infrastructure of the System will be shared between Member Agencies as indicated in the SBISS South Bay Region Node Share of Cost Agreement and approved by Board of Directors. In the event that hardware or software upgrades are required to facilitate the proper functioning of the system, the Board of Directors will notify the Member Agency in writing at least ninety (90) days in advance of the funding requirement.

7.4 Grant Funding: Grant funding provided by the Urban Area Security Initiative, Homeland Security Grant Program, Federal Emergency Management Agency, U.S. Department of Homeland Security has been used to offset the start-up costs for the Node. The primary use of these funds will focus on infrastructure, paying for software license maintenance, and data integration fees for the Member Agencies. The Fiscal Agent will manage all aspects of payment and reporting for grant funding.

7.5 Future Grant Funding: Member Agencies that individually apply for grant funding for this system should notify the South Bay Region Node Board of Directors to avoid duplicative efforts and requests for funding. Any grant funding which may result from such applications will be considered to be outside of this MOU. The Member Agencies may choose to apply

jointly for grant funding and upon the written agreement of the Member Agencies; such monies shall fall under the jurisdiction of this MOU.

7.6 Member Agency Employees: Employees of a Member Agency working for the benefit of the Node remain the employees of that Member Agency.

8 Amendments

8.1 Addition of new Member Agencies: If additional agencies choose to become Member Agencies after this MOU is executed, this Agreement shall be amended to include those agencies as signatories.

8.2 This MOU may be modified by presentation of the proposed changes and an affirmative majority vote of the Board.

8.3 All approved amendments must be in writing and approved by the Board.

9 Termination

9.1 MOU Termination: This MOU may be terminated by mutual agreement of all Member Agencies.

9.2 Member Agency Termination: Any Member Agency may terminate its participation in this MOU with or without cause upon sixty-days (60) prior written notice to the Board, unless such termination is prohibited by a grant condition or unless the Member Agency is a Host Node. If the Member Agency wishes to remove Data from the Node after terminating its participation, that Member Agency will be responsible for any costs associated with removing their Data from the Node.

Other Termination: The Board may exercise its authority to terminate the relationships established under this MOU if the majority members of the Board determine that a Member Agency is not complying with the terms and conditions of this MOU, the Cost Sharing Agreement (Exhibit A); and/or the System Use Policy (Exhibit B).

10 Miscellaneous

10.1 This MOU is intended to provide for a strategic plan to promote data sharing and should be amended as necessary to accomplish the goal of

fully integrating the Member Agencies, future agencies and potential future data sources.

10.2 From time to time the Member Agencies may develop, adopt or create additional policies and/or procedures related to other forms of information gathering and sharing, hosted by SBISS. The Member Agencies will have an opportunity to review, comment or revise these policies and once approved by the Board of Directors, the policies will be incorporated herein (See, Appendix) and the Member Agencies will be bound by the terms therein.

The parties hereto execute this MOU as of the Effective Date.

Santa Clara County Agencies:

City of Campbell

_____ _____
Mark Linder Date
City Manager
City of Campbell

_____ _____
Greg Finch Date
Chief of Police
City of Campbell

City of Gilroy

_____ _____
Thomas J. Haglund Date
City Manager
City of Gilroy

_____ _____
Denise J. Turner Date
Chief of Police
City of Gilroy

City of Los Altos

_____ _____
Marcia Somers Date
City Manager
City of Los Altos

_____ _____
Tuck Younis Date
Police Chief
City of Los Altos

Town of Los Gatos

_____ _____
Greg Larson Date
Town Manager
Town of Los Gatos

_____ _____
Scott Seaman Date
Police Chief
Town of Los Gatos

City of Milpitas

_____ _____
Thomas C. Williams Date
City Manager
City of Milpitas

_____ _____
Steve Pangelinan Date
Police Chief
City of Milpitas

City of Morgan Hill

_____ _____
Steve Rymer Date
City Manager
City of Morgan Hill

_____ _____
David Swing Date
Police Chief
City of Morgan Hill

City of Mountain View

_____ _____
Daniel H. Rich Date
City Manager
City of Mountain View

_____ _____
Scott S.G. Vermeer Date
Police Chief
City of Mountain View

City of Palo Alto

_____ _____
Jim Keene Date
City Manager
City of Palo Alto

_____ _____
Dennis Burns Date
Police Chief
City of Palo Alto

City of San Jose

_____ _____
Ed Shikada Date
City Manager
City of San Jose

_____ _____
Larry Esquivel Date
Police Chief
City of San Jose

San Jose State University

_____ _____
Date

Administration and Finance
San Jose State University

_____ _____
Peter Decena Date
Police Chief
San Jose State University

City of Santa Clara

_____ _____
Julio J. Fuentes Date
City Manager
City of Santa Clara

_____ _____
Mike Sellers Date
Police Chief
City of Santa Clara

County of Santa Clara

_____ _____
Jeffrey Smith M.D. Date
County Executive
County of Santa Clara

_____ _____
Laurie Smith Date
Sheriff
County of Santa Clara

_____ _____
Karen Fletcher (Interim) Date
Chief Probation Officer
County of Santa Clara

_____ _____
Jeffrey Rosen Date
District Attorney
County of Santa Clara

City of Sunnyvale

_____ _____
Gary Luebbers Date
City Manager
City of Sunnyvale

_____ _____
Frank Grgurina Date
Director of Public Safety
City of Sunnyvale

Santa Cruz County Agencies:

City of Capitola

_____ _____
Jamie Goldstein Date
City Manager
City of Capitola

_____ _____
Rudy Escalante Date
Chief of Police
City of Capitola

City of Santa Cruz

_____ _____
Martin Bernal Date
City Manager
City of Santa Cruz

_____ _____
Kevin Vogel Date
Chief of Police
City of Santa Cruz

County of Santa Cruz

_____ _____
Susan A. Mauriello Date
County Administrative Officer
County of Santa Cruz

_____ _____
Phil Wowak Date
Sheriff-Coroner
County of Santa Cruz

_____ _____
Scott MacDonald Date
Chief Probation Officer
County of Santa Cruz

_____ _____
Bob Lee Date
District Attorney
County of Santa Cruz

City of Watsonville

_____ _____
Carlos J. Palacios Date
City Manager
City of Watsonville

_____ _____
Manny Solano Date
Police Chief
City of Watsonville

Monterey County Agencies:

City of Carmel

_____ _____
Jason Stilwell Date
City Administrator
City of Carmel

_____ _____
Mike Calhoun Date
Police Chief
City of Carmel

City of Del Rey Oaks

_____ _____
Daniel Dawson Date
City Manager
City of Del Rey Oaks

_____ _____
Ronald J. Langford Date
Chief of Police
City of Del Rey Oaks

City of Gonzales

_____ _____
Rene L. Mendez Date
City Manager
City of Gonzales

_____ _____
Paul Miller Date
Police Chief
City of Gonzales

City of Greenfield

_____ _____
Susan Stanton Date
City Manager
City of Greenfield

_____ _____
Bradley W. Sullivan Date
City Attorney
City of Greenfield

_____ _____
Adele H. Frese Date
Police Chief
City of Greenfield

City of King City

_____ _____
Michael Powers Date
City Manager
City of King City

_____ _____
Bruce Miller (Interim) Date
Police Chief

City of Marina

_____ _____
Layne P. Long Date
City Manager
City of Marina

_____ _____
Edmundo Rodriquez Date
Chief of Police
City of Marina

City of Monterey

_____ _____
Fred Meurer Date
City Manager
City of Monterey

_____ _____
Phil Penko Date
Chief of Police
City of Monterey

City of Pacific Grove

_____ _____
Thomas Frutchey Date
City Manager
City of Pacific Grove

_____ _____
Vicki L.H. Myers Date
Police Chief
City of Pacific Grove

City of Salinas

_____ _____
Ray Corpuz Date
City Manager
City of Salinas

_____ _____
Kelly McMillin Date
Police Chief
City of Salinas

City of Sand City

_____ _____
Todd Bodem Date
City Administrator
City of Sand City

_____ _____
Brian Ferrante Date
Police Chief
City of Sand City

City of Seaside

_____ _____
John Dunn Date
City Manager
City of Seaside

_____ _____
Vicki L.H. Myers Date
Police Chief
City of Seaside

County of Monterey

_____ _____
Lew C. Bauman Date
County Administrative Officer
County of Monterey

_____ _____
Stephen T. Bernal Date
Sheriff
County of Monterey

_____ _____
Manuel Real Date
Chief Probation Officer
County of Monterey

_____ _____
Dean D. Flippo Date
District Attorney
County of Monterey

City of Soledad

_____ _____
Adela P. Gonzalez Date
City Manager
City of Soledad

_____ _____
Eric Sills Date
Chief of Police
City of Soledad

California State University, Monterey Bay

_____ _____
Kevin Saunders Date
VP Administration and Finance
California State University, Monterey Bay

_____ _____
Earl Lawson Date
Chief of Police
California State University, Monterey Bay

San Benito County Agencies:

City of Hollister

_____ _____
Clint Quilter Date
City Manager
City of Hollister

_____ _____
Dave Westrick Date
Police Chief
City of Hollister

County of San Benito

_____ _____
Ray Espinosa Date
County Administrative Officer
County of San Benito

_____ _____
Darren Thompson Date
Sheriff-Coroner
County of San Benito

_____ _____
Don H. Blevins (Interim) Date

Chief Probation Officer
County of San Benito

_____ _____
Candice Hooper Date
District Attorney
County of San Benito

_____ _____
Date

_____ _____
Date

_____ _____
Date

_____ _____
Date

EXHIBIT A
SHARE OF COST AGREEMENT
South Bay Information Sharing System (SBISS)
SOUTH BAY REGION NODE

Purpose and Background
The Santa Clara County Sheriff's Office and Member Agencies agree to the terms and conditions set forth in the South Bay Information Sharing System (SBISS). SBISS is overseen by the South Bay Information Sharing System Board of Directors. Agencies enter into this cost sharing agreement to participate in the information-sharing system known as COPLINK via the South Bay Region Node. This agreement outlines the financial working relationship and cost-sharing contract for South Bay Region Node member agencies.

THEREFORE, the Member Agencies herby agree to the following:

1 Definitions

1.1 **South Bay Information Sharing System (SBISS)** is the name of the information sharing system node hosted by the Santa Clara County Office of the Sheriff.

1.2 **South Bay Information Sharing System (SBISS) Board of Directors** is the governing body of the South Bay Information Sharing System.

1.3 **Data** shall mean electronic facts, detailed information, or other material provided by a Member Agency.

1.4 **Data Repository** shall mean the computer equipment used to store, connect and disseminate data sharing information to Member Agencies.

1.5 **The Santa Clara County Office of the Sheriff** is the fiscal agent for the South Bay Region Node of SBISS and will handle and account for funds collected by the Node for the benefit of all Member Agencies.

1.6 **South Bay Region Node** shall mean the collective signatory law enforcement and justice agencies, within Santa Clara, Santa Cruz, Monterey and San Benito Counties who have agreed to work within the parameters of this Agreement.

1.7 **South Bay Region Node** is the collective group of agencies that have entered into a MOU agreement to participate in the SBISS South Bay Region Node for law enforcement information-sharing.

1.8 **Member Agency** shall mean law enforcement agencies contributing data to the South Bay Region Node SBISS, including District Attorney or University Police Member agencies and allowed access to data of other member agencies and other COPLINK nodes.

1.9 **International Business Machines** (IBM) shall mean a corporation with its principal place of COPLINK business at 1 New Orchard Road, Armonk, New York,10504-1722, and the owner and developer of COPLINK.

1.10 **COPLINK** shall mean the information sharing and analysis software licensed to the member agencies by IBM under the name COPLINK.

1.11 **Vendor Tools** shall mean the SBISS information sharing and analysis software available to the member agencies.

2 Requirements for Participation

2.1 To participate in the South Bay Region Node, Member Agencies agree to share costs based on the "member population" computation as described in Section 4 below. Other cost sharing formulas may be proposed and considered by the South Bay Region Node Board of Directors when the MOU is renewed or amended.

2.2 To participate in the South Bay Region Node, Member Agencies agree to contribute data from their Records Management System (RMS), Jail Management System (JMS), Mugshot or Case Management System (CMS) , and law enforcement data as defined by the South Bay Region Node Technology Committee.

3 Financial Oversight and Management

3.1 **Node Costs**: After the current Grant Funding is exhausted in 2015, Member Agencies shall pay a proportional share of software purchase costs, software maintenance, implementation, network, hardware, and operational costs, as approved by the South Bay Region Node as approved by the SBISS Board of Directors.

3.2 **Annual Budget** Each year the Santa Clara County Office of the Sheriff shall prepare an annual budget for approval by the Board of Directors that identifies the expenses each Member Agency will be required to contribute for the year.

3.3 **Annual Report** At least once a year the Santa Clara County Office of the Sheriff shall report to the SBISS Board of Directors on all funds

collected and expended by the South Bay Region Node in support of the COPLINK project.

3.4 **Payment Administration** The Santa Clara County Office of the Sheriff shall administer payments to all vendors and invoice Member Agencies for their share of this cost.

3.5 **Financial Responsibility** The Santa Clara County Office of the Sheriff will be responsible for paying for the expenses associated with connecting to the SBISS Node data repository, which may include acquiring hardware, software, data communication equipment and/or other required services. For any expenses incurred before January 1, 2015, the Santa Clara County Sheriff's Office will use the funds received from grant awarded by the U.S. Department of Homeland Security. After January 1, 2015, the Member Agencies shall be responsible for paying for those costs related to maintenance and upgrades to the system unless covered by grant funding. No Member Agency shall be responsible for funding the activities of any other Member Agency.

3.6 **Payment Schedule**

Homeland Security Grant Program: The UASI grants from the U.S. Department of Homeland Security has paid for the necessary hardware infrastructure for the South Bay Region Node, 100% of the data integration costs for each Member Agency, the enterprise software license fee, and three years of maintenance. The following chart outlines the initial and ongoing maintenance costs for Member Agencies to participate in the SBISS Node including those expenses not covered by the grant. These maintenance costs are subject to review and additional assessment by the SBISS South Bay Regional Node Board of Directors. Additional Homeland Security grant funding has been secured with Fiscal Years 2010, 2011, 2012 and 2013 funding related to sustainment and enhancements to the sharing system. Please refer to cost sharing allocation tables below. Table 1 is the current cost sharing model applicable to the "Original Member Agencies" and "University Police Member Agencies", while Tables 2 and 3 apply to "New Member Agencies" that consist of the SBISS Region Probation Departments from Santa Clara, Santa Cruz, Monterey and San Benito counties.

Table 1

Agency	2010 Population	% of Total Population	Cost Allocation Years 2, 3, & 4[2]	Cost Allocation Starting Year 5[3] (Jan 1, 2015)
Santa Clara County				
Campbell PD	39,349	2.16%	$ 1,198.61	$ 3,576.91
Gilroy PD	48,821	2.68%	$ 1,487.14	$ 4,437.93
Los Altos PD	28,976	1.59%	$ 882.64	$ 2,633.98
Los Gatos PD plus Monte Sereno	32,754	1.80%	$ 997.72	$ 2,977.41
Milpitas PD	66,790	3.67%	$ 2,034.50	$ 6,071.35
Morgan Hill PD	37,882	2.08%	$ 1,153.93	$ 3,443.55
Mountain View PD	74,066	4.07%	$ 2,256.13	$ 6,732.76
Palo Alto PD	64,403	3.54%	$ 1,961.79	$ 5,854.37
San Jose PD	958,966	52.68%	$ 29,211.17	$ 87,172.06
San Jose State Univ PD	24,048	1.32%	$ 732.53	$ 2,186.01
Santa Clara PD	116,468	6.40%	$ 3,547.74	$ 10,587.19
Sheriff Unincorporated plus: (Cupertino,Saratoga, Los Altos Hills)	187,747	10.31%	$ 5,718.98	$ 17,066.60
Sunnyvale DPS	140,081	7.70%	$ 4,267.02	$ 12,733.66
Total Santa Clara County	**1,820,351.00**	**100%**	**$ 55,449.91**	**$ 165,473.79**
Santa Cruz County				
Capitola PD	9,918	4.02%	$ 302.11	$ 1,156.70
Santa Cruz PD	59,946	24.28%	$ 1,826.02	$ 6,991.29
Scotts Valley (11,580 population)	0	0.00%	$ -	$ -
Sheriff	125,831	50.97%	$ 3,832.95	$ 14,675.22
Watsonville PD	51,199	20.74%	$ 1,559.58	$ 5,971.16
Total Santa Cruz County	**246,894**	**100%**	**$ 7,520.67**	**$ 28,794.36**
Monterey County				
Carmel PD	3,722	0.88%	$ 113.38	$ 625.26
Del Rey Oaks -(1,624 population)	0	0.00%	$ -	$ -
Gonzales PD	8,187	1.94%	$ 249.39	$ 1,375.33
Greenfield PD	16,330	3.87%	$ 497.43	$ 2,743.26
King City PD	12,874	3.05%	$ 392.16	$ 2,162.69
Marina PD	19,718	4.68%	$ 600.63	$ 3,312.41
Monterey	27,810	6.60%	$ 847.12	$ 4,671.78
Pacific Grove	15,041	3.57%	$ 458.17	$ 2,526.72
Salinas	150,441	35.70%	$ 4,582.60	$ 25,272.45

Sand City	334	0.08%	$ 10.17	$ 56.11
Seaside	33,025	7.84%	$ 1,005.98	$ 5,547.84
Sheriff	101,208	24.02%	$ 3,082.91	$ 17,001.84
Soledad	25,738	6.11%	$ 784.01	$ 4,323.70
California State University Monterey Bay	7,000	1.66%	$ 213.23	$ 1,175.92
Total Monterey County	**421,428.00**	**100%**	**$ 12,837.17**	**$ 70,795.32**
San Benito County				
Hollister	34,928	64.98%	$ 1,063.95	$ 7,770.26
Sheriff	18,821	35.02%	$ 573.31	$ 4,187.02
Total San Benito County	**53,749.00**	**100%**	**$ 1,637.25**	**$ 11,957.28**
Total annual maintenance all counties			**$ 77,445.00**	**$ 277,020.76**

Table 1 Notes:

[1] The population is based on the 2010 census data and will provide the basis for initial cost sharing along with agency sworn counts. Percentages in table 1 are determined by the total covered population for respective agency as a portion of total County population. Sworn counts are based on California POST Statistics for Current Employed Full-Time Sworn and determine SBISS license costs as a percentage of total State sworn counts.

[2] Cost allocation Years 2, 3, and 4 represent: Year 2: (10/01/11 to 9/30/12), Year 3: (10/01/12 to 12/31/13), and Year 4: (01/01/14 to 12/31/14. The expenses allocated during these periods include but are not limited to the Host and Resource Annual costs associated with a .5 FTE Information Systems Staff.

[3] Cost allocation begins in Year 5 – January 1, 2015. The expenses allocated during this period include but are not limited to the COPLINK annual software and Integration Services Maintenance & Technical Support license fee and the Host and Resource Annual costs that include network hardware, Internet Services maintenance and the costs associated with a .5 FTE Information Systems Staff.

Table 2

SBISS (Probation Module) Licensing, Integration and Support Costs (Summary)	Probation Costs
SMRA MODULE Cost **($99,500.00: Paid with Grant Funding)**	**Grant Funded**
Integration Cost **($37,672.00: Paid with Grant Funding)**	**Grant Funded**
SUBTOTAL ($137,172.00)	**Grant Funded**
Year 1- Host Site Costs (Paid for by each Probation Dept.)	**$ 2,100.00**
Year 1- License Maintenance Costs (Divided by Participating Probation Depts.)	**Grant Funded**
Year 1- Integration Maintenance Costs (Paid for by each Probation Dept.)	**Grant Funded**
Year 2- Host Site Costs (Paid for by each Probation Dept.)	**$ 2,100.00**
Year 2- License Maintenance Costs (Shared by Participating Probation Depts.)	**Grant Funded**
Year 2- Integration Maintenance Costs (Paid for by each Probation Dept.)	**Grant Funded**
Year 3- Host Site Costs (Paid for by each Probation Dept.)	**$ 2,100.00**
Year 3- License Maintenance Costs (Shared by Participating Probation Depts.)	**$ 12,935.00**
Year 3- Integration Maintenance Costs (Paid for by each Probation Dept.)	**$ 4,897.36**

Table 3

COPLINK SRMA (PROBATION MODULE) Annual Software & Integration Services Maintenance & Support				
[Item 1]: Probation Module (Grant Funded)				$ 99,500.00
[Item 2]: Probation Integration Costs for Each Department (Grant Funded)				$ 37,672.00
[Item 3]: Software License Annual Maintenance (@ 13%)				$ 12,935.00
[Item 4]: Integration Annual Maintenance (@ 13%)				$ 4,897.36
Santa Clara County - Probation	**Year 1 [a]**	**Year 2 [b]**	**Year 3 [c]**	**Cost Details**
Host Site	$ 2,100.00	$ 2,100.00	$ 2,100.00	$ 2,100.00
Software Maintenance	Grant Funded	Grant Funded	$ 3,233.75	$ 3,233.75
Integration Maintenance	Grant Funded	Grant Funded	$ 4,897.36	$ 4,897.36
Total - Santa Clara County (grant coverage until 6/30/15)	$ 2,100.00	$ 2,100.00	$ 10,231.11	$ 10,231.11
Santa Cruz County - Probation	**Year 1 [a]**	**Year 2 [b]**	**Year 3 [c]**	**Cost Details**
Host Site	$ 2,100.00	$ 2,100.00	$ 2,100.00	$ 2,100.00
Software Maintenance	Grant Funded	Grant Funded	$ 3,233.75	$ 3,233.75
Integration Maintenance	Grant Funded	Grant Funded	$ 4,897.36	$ 4,897.36
Total - Santa Cruz County (grant coverage until 6/30/15)	$ 2,100.00	$ 2,100.00	$ 10,231.11	$ 10,231.11
Monterey County - Probation	**Year 1 [a]**	**Year 2 [b]**	**Year 3 [c]**	**Cost Details**
Host Site	$ 2,100.00	$ 2,100.00	$ 2,100.00	$ 2,100.00
Software Maintenance	Grant Funded	Grant Funded	$ 3,233.75	$ 3,233.75
Integration Maintenance	Grant Funded	Grant Funded	$ 4,897.36	$ 4,897.36
Total - Monterey County (grant coverage until 6/30/15)	$ 2,100.00	$ 2,100.00	$ 10,231.11	$ 10,231.11
San Benito County - Probation	**Year 1 [a]**	**Year 2 [b]**	**Year 3 [c]**	**Cost Details**
Host Site	$ 2,100.00	$ 2,100.00	$ 2,100.00	$ 2,100.00
Software Maintenance	Grant Funded	Grant Funded	$ 3,233.75	$ 3,233.75
Integration Maintenance	Grant Funded	Grant Funded	$ 4,897.36	$ 4,897.36
Total – San Benito County (grant coverage until 6/30/15)	$ 2,100.00	$ 2,100.00	$ 10,231.11	$ 10,231.11

[a] Year 1 (7/01/13 - 6/30/14): Host site costs apply during year one and commence after implementation is complete.
[b] Year 2 (7/01/14 - 6/30/15): Grant Funding for software and integration maintenance. Excludes host site costs.
[c] Year 3 (7/01/15 - 6/30/16): To include software and integration maintenance along with host site costs.
[Item 3] Should a Probation Department determine not to continue after the completion of one year, then the remaining Departments would be responsible for sharing licensing costs for item 3. SBISS will plan to include the above costs for all future grant requests excluding host site costs. *Note: Annual Billing: Billing invoices related to host site costs will be sent during the last quarter of the first year. After the successful implementation of the module and integration of the final probation case management system, the maintenance cycle will commence. After the first annual cycle completes, Probation Departments will be responsible for sustainment of the probation module, and datasource integration maintenance. Currently host site costs

have not been eligible for grant funding coverage and as a result, member agencies have had to include these costs as part of their annual budgets.

Table 4

Annual Support			
District Attorney	**Sworn Count**	***Network, Administration and Training Resource Hours**	**Annual Support**
Agency A	1-19	10	$ 1,032.70
Agency B	20-30	20	$ 2,065.40
Agency C	31-50	30	$ 3,098.10
Agency D	50 plus	50	$ 5,163.50
***Account creation and administration, network connectivity and security, training and travel, and phone support.**			

3.7 Agency annual maintenance costs for items not covered by the grant will begin at the soonest on July 1, 2010. Each year the fiscal agent will invoice each Member Agency for the maintenance costs. The member Agency shall pay the annual payment within 30 days of receipt. If payment or payment arrangements have not been agreed to by the payment due date, services will be terminated.

3.8 Each Member shall pay a share of the Annual Maintenance Costs based on the principle that Members shall share the systems maintenance costs based on the system, sworn counts (Table 5), and member population computation or other on-going cost computation as determined by the South Bay Region Node Board of Directors. Member Agency population was based on the 2010 U. S. Census and will be updated to reflect the 2010 U.S Census numbers.

Including sworn counts, the cost allocations for each police department and Sheriff's Office will reflect the U. S. Census data with the exception that Los Gatos-Monte Sereno Police Department will be assessed the combined population allocations for the City of Los Gatos and the City of Monte Sereno and the assessment for the Santa Clara County Office of the Sheriff will be the combined population allocations for the unincorporated Santa Clara County, the City of Cupertino, the City of Saratoga, and the City of Los Altos Hills. Additionally, the District Attorney member agencies will have cost sharing allocations specific to their agencies and are reflected in above tables 4 and 5 respectively. The other exception is for all University Police Departments as their allocations will be based on campus populations.

Table 5

County	Agency Name	New
Santa Clara	Campbell	41
	Gilroy	59
	Los Altos	30
	Los Gatos	38
	Milpitas	75
	Morgan Hill	36
	Mountain View	95
	Palo Alto	79
	San Jose	1045
	San Jose Univ PD	27
	Santa Clara PD	134
	Santa Clara SO	453
	Sunnyvale	200
Santa Cruz	Capitola PD	21
	Santa Cruz PD	87
	Santa Cruz SD	137
	Watsonville PD	67
Monterey	Carmel PD	14
	CSU Monterey Bay	15
	Gonzales PD	11
	Greenfield PD	14
	King City PD	15
	Marina DPS	34
	Monterey PD	48
	Monterey SD	287
	Pacific Grove PD	16
	Salinas PD	148
	Sand City PD	10
	Seaside PD	37
	Soledad PD	16
San Benito	Hollister PD	21
	San Benito SD	21
	Total	**3331**

POST Statistics Current Employed Full-Time Sworn:
(http://www.post.ca.gov/Data/Sites/1/post_docs/hiring/le-employment-stats.pdf

Cost allocation for the Probation Departments (see above Table 3) will be based on shared maintenance costs for sustainment of the COPLINK Supervised Release and Monitoring Alert Module (SRMA Module), and the integration of their respective case management data source into COPLINK data warehouse.

Cost allocation for the District Attorney Offices will be based on sworn counts (see above Table 4).

3.9 In the event of a violation of the terms and conditions of the Cost Sharing Agreement, the Board will be responsible for analyzing any violation of the Agreement and will determine what action, if any shall be taken against the Member Agency for said violation.

EXHIBIT C

EMPLOYEE/VOLUNTEER STATEMENT FORM

As an employee/volunteer of _____, you may have access to confidential records stored in the SBISS South Bay Information Sharing System. All access is based on the "need to know" and the "right to know." Misuse of such information may adversely affect an individual's civil rights, and violates the law and/or SBISS policy.

Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11141-11143 and 13302-13304 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records.

"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information not authorized by law to receive the record or information is guilty of a misdemeanor."

Any employee/volunteer who is responsible for SBISS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE RECEIVED A COPY OF THE TERMS AND CONDITIONS OF USAGE OF COPLINK. I AGREE TO COMPLY WITH THE TERMS AND CONDITIONS AND I UNDERSTAND THAT VIOLATION OF ANY OF THE TERMS AND CONDITIONS MAY LEAD TO DISCIPLINARY ACTION AND OR CRIMINAL PROSECUTION

_____

Signature Print Name

Date _____

Exhibit D

COPLINK

ANNUAL DATA AUDIT FOR DATA ACCURACY

Date	Time	Data Type	Data	Verified in COPLINK?

Appendix

Table of Contents

I. Policies and Procedures
    1. *South Bay Information Sharing System ALPR Policies and Procedures*; Incorporated 8/29/13

MEMORANDUM OF UNDERSTANDING

This Data Sharing Memorandum of Understanding (hereinafter "**MOU**") is entered into by and between Flock Group, Inc. with a place of business at 2588 Winslow Drive, Atlanta, GA 30305 ("**Flock**") and Massachusetts State Police with a place of business at 470 Worcester Road, Framingham, Massachusetts 01702 ("**Agency**") (each a "**Party**", and together, the "**Parties**").

Whereas, Agency desires to access Flock's technology platform and Flock Safety dashboard (together, the "**Flock Service**") for investigative purposes, in order to view and search videos recorded by Flock ("**Recordings**") which are stored for no longer than thirty (30) days, utilizing its software for automatic license plate detection;

Whereas, Flock desires to share such videos and supplemental data with Agency pursuant to the following terms and conditions:

1. **Purpose**. To allow the Agency to utilize the Flock Services for the following purpose: to gain awareness with respect to the communities for which they serve to protect and facilitate investigations (the "Purpose").

2. **Access Rights to Flock Services**. Subject to the terms and conditions contained in this MOU, Flock hereby grants to Agency a non-exclusive, non-transferable right to access the features and functions of the Flock Service during the Term (as defined below), solely for use by Authorized Users in accordance with the terms and conditions herein. For purposes of this MOU, "Authorized Users" will mean employees, agents, or officers of Agency accessing or using the Flock Services for the Purpose. Agency acknowledges and agrees that, as between Agency and Flock, Agency shall be responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User which would constitute a breach of this MOU, shall be deemed a breach of this MOU by Agency. Agency shall undertake reasonable efforts to make all Authorized Users aware of the provisions of this MOU as applicable to such Authorized User's use of the Flock Service, and shall cause Authorized Users to comply with such provisions.

3. **Restrictions on Use**. Agency will not, and will not permit any Authorized Users or any third party to, (i) copy or duplicate any of the Flock Service; (ii) decompile, disassemble, reverse engineer or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock Service is compiled or interpreted; (iii) modify, alter, or tamper with any of the Flock Service, or create any derivative product from any of the foregoing; (iv)

interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock Service; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within any of the Flock Service; or (vi) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Agency's rights under Sections 2. Agency may only access Recordings and Flock Service to perform the Purpose, as described in Section 1. Agency shall not use the Flock Service in any manner not permitted by appropriate governing Federal and State regulations or laws; Agency represents and warrants that, in receiving access to Flock Services, such video and supplemental data shall be used solely for purposes authorized by law and described in this MOU.

4. **Ownership**. As between the Parties, subject to the rights granted in this MOU, Flock and its licensors retain all right, title and interest in and to the Flock Service, and its components and any Recordings or data provided by Flock through the Flock Service, and Agency acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this MOU. Agency further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. There are no implied rights.

5. **Warranty**. Flock and its licensors make no express or implied warranty as to the conditions of the Recordings, or fitness for a particular research, data, investigative purpose or resulting actions or omissions resulting from videos and supplemental data obtained by Agency through the use of Flock Services.

6. **Financial Implications to Agency**. No financial commitment by Agency is required to access the Flock Services or Recordings.

7. **Term; Termination**.

A. **Term**. This MOU will commence once executed by both parties and shall continue for a period of Five (5) years.

B. **Termination**. Prior to expiration of the Term, Flock may terminate this MOU for its convenience, and in its sole discretion, by providing Agency thirty (30) days prior written notice of termination. Agency may terminate this MOU for its convenience, and in its sole discretion, by providing Flock ninety (90) days prior written notice of termination. Either party may terminate this MOU upon written notice if the other party has breached a material term of this MOU and has not cured such breach within thirty (30) days of receipt of notice from the non-breaching party specifying the breach. Upon termination of this MOU, Agency will

immediately cease all use of Flock Services. This MOU is subject to termination without written notice after expiration of the Term.

8. **Indemnification**. Each Party to this MOU shall assume the responsibility and liability for the acts and omissions of its own employees, deputies, officers, or agents, in connection with the performance of their official duties under this MOU. Parties shall indemnify and hold harmless each other against any suits, claims, actions, complaints, or liability of any kind, which relate to the use of or reliance on Flock Service. For tort liability purposes, no participating Party shall be considered the agent of the other participating Party. Each Party to this MOU shall be liable (if at all) only for the torts of its own officers, agents, or employees that occur within the scope of their official duties. Under no circumstances shall this MOU be interpreted to create a partnership or agency relationship between the Parties.

9. **Limitation of Liability**.

A. Limitation on Direct Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL FLOCK, ITS OFFICERS, DIRECTORS, AGENTS, EMPLOYEES OR REPRESENTATIVES BE LIABLE FOR ANY AMOUNT GREATER THAN THE FEES PAID TO FLOCK UNDER THIS MOU, OR $100 IN UNITED STATES CURRENCY, WHICHEVER IS GREATER, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), PRODUCT LIABILITY OR OTHERWISE.

B. Waiver of Consequential Damages. IN NO EVENT SHALL FLOCK OR ITS LICENSORS OR SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA OR LOSS OF PROFITS, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

10. **Confidentiality**.

A. **Obligations**. During the performance of services and Agency's use of the Flock Service under this Agreement it may be necessary for a party to provide the other with certain information considered to be proprietary or confidential by the disclosing party. The disclosure of such confidential information shall be subject to the following terms and conditions.

i. The term "Agency Confidential Information" shall mean any material, data, systems, procedures and other information of or with respect to Agency that is not be accessible or known to the general public, including information concerning its hardware, software, business plans or opportunities, business strategies, finances, employees, and third-party proprietary or other information that Agency treats as confidential. Flock shall not use, publish or divulge any Agency Confidential Information except (i) in connection with Flock's provision of Software and services pursuant to this Agreement, (ii) to Flock's officers, directors, employees, agents and contractors who need to know such information to enable Flock to provide Software and services pursuant to this Agreement, or (iii) with the prior written consent of Agency, which consent Agency may withhold in its sole discretion.

ii. The term "Flock Confidential Information" means any material, data, systems, procedures and other information of or with respect to Flock that is not accessible to or known to the general public, including, without limitation, the software, object code, source code, formulae, algorithms, financial data, clients, employees, software development plans, software support third-party proprietary or other information that Flock treats as confidential. Agency shall not use, publish or divulge any Flock Confidential Information except (i) to its employees, agents and officers who need to know such information to enable Agency to use the Flock Services, or (ii) with the prior written consent of Flock, which consent Flock may withhold in its sole discretion.

iii. Each party shall protect the other's confidential information with the same degree of care normally used to protect its own similar confidential information, but in no event less than that degree of care that a reasonably prudent business person would use to protect such information. The obligations of each party to protect confidential information received from the other party shall not apply to information that is publicly known or becomes publicly known through no act or failure to act on the part of the recipient. All provisions of this MOU concerning the Confidentiality section herein, shall survive any termination of this MOU.

B. **Exclusions**. Confidential Information shall not include any information that is (i) already known to the receiving party at the time of the disclosure; (ii) publicly known at the time of the disclosure or becomes publicly known through no wrongful act or failure of the receiving party; (iii) subsequently disclosed to the receiving party on a non-confidential basis by a third-party not having a confidential relationship with the other party hereto that rightfully acquired such information; or (iv) communicated to a third party by the receiving party with the express written consent of the other party hereto. A disclosure of Confidential Information that is legally compelled to be disclosed pursuant to a subpoena, summons, order or other judicial or governmental process or the Freedom of Information Act shall not be considered a breach

of this MOU; provided the receiving party provides prompt notice of any such subpoena, order, or the like to the other party so that such party will have the opportunity to obtain a protective order or otherwise oppose the disclosure.

11. **Entire Agreement**. This MOU is complete and contains the entire understanding between the Parties relating to the sharing of Recordings and Confidential Data by and between Flock and Agency. This MOU supersedes any and all other agreements between the Parties. This Agreement is non-assignable by both Parties.

12. **Severability**. Nothing is this MOU is intended to conflict with or violate State or Federal laws, regulations, policies, etc. If a term or provision of this MOU is inconsistent with a law or authority, then that term or provision shall be invalid, but the remaining terms and provisions shall remain in full force and effect. If any provision of this MOU is found to be unenforceable, unlawful, or void, the provision shall be deemed severable from the MOU and shall not affect the validity of the remaining provisions.

13. **Miscellaneous**. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission To the facsimile number below and indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. This MOU shall be governed by the laws of the state in which the Agency is located, excluding its conflict of laws rules. The parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this MOU.

IN WITNESS WHEREOF, Flock and the Agency have caused this MOU to be signed on the date set forth below and be effective on the last date specified below.

FLOCK GROUP, INC.	**Massachusetts State Police**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

MSP Sample Camera - IP SCHEMA (CAMNET)

NOTES: ie Server Serial Number (DELL TAG), misc equipment (switches, monitors)

Credentia
Servers:
Workstatio
Cameras:
Wireless:

Subnet:
Gateway:
NTP:

IP Address	Device #	Make & Model	FW Version	MAC Address	Credentials	Switch/
[redacted]	Avigilon Server NIC 1	[redacted]				1
	Avigilon Server NIC 2					2
	Workstation 1					3
	Workstation 2					4
	7					5
	12					6
	25					7
	8					8
	9		1			9
	26		1			10
	2					11
	14		1			12
	3					13
	15		1			14
	16		2			15
	17					16
	13					17
	10					18
	18					19
	19					20
	5					21
	20					22
	21					23
	11					24
	22					25

[redacted]	6	[redacted]	4			26
	23		4			27
	24		4			28
	CPE 1					29
	CPE 2					30
	CPE 3					31
	CPE 4					32
	AP 1					33
	AP 2					34
						35
						36
						37
						38
						39

ls
ns:

/Port	Camera Name

Norfolk District Attorney's Office
Digital Evidence & Search Warrant Update

In recent years, Massachusetts courts have expanded protections afforded to suspects in the context of search and seizure of digital evidence. This handout provides general guidance as of June 1, 2022 for the drafting of search warrants for digital evidence based on recent case law, "best practices" and emerging trends.

OVERVIEW

- If you are unsure if you need a search warrant, the answer is likely **YES.**
- Prior to obtaining search warrant learn through investigation, interviews, open source materials: phone number, type of phone, network, whether phone has passcode, whether suspect knows passcode, who is phone registered to, type of communication involved, when communication occurred, any video of suspect using phone, location of phone before, during and after crime, suspect's social media account names, contact names, etc… Do not manipulate a phone to obtain this information.
- Search warrants should be structured to contain: 1) affiant training and experience; 2) summary of investigation/specific facts of case; 3) reasonable inferences; 4) basis for probable cause; 5) narrowly tailored and time limited request to search item for specific evidence of a crime.
- A well-written affidavit is essential for successful prosecution. To avoid suppression of key evidence, fully explain why probable cause exists, what evidence supports your opinions, and what inferences can be drawn based on the facts of your case, even if they seem obvious.
- Articulate probable cause for all crimes.
- Avoid asking to search "any and all . . ." or "including but not limited to…." This may be construed as an overbroad search.
- Avoid saying, "I believe that evidence of [CRIME] may be found of the device," instead say "There is probable cause that evidence of [CRIME] will be found on the device."
- Please reach out to the Norfolk District Attorney's Office [NDAO] at (781) 830-4800 with any specific questions. There are ADAs available to review warrants before submission to the judge/clerk magistrate.
- The Norfolk District Attorney's Office has a Digital Forensics Division available to conduct the forensic examination of digital devices. Please contact Director Samantha Vogt at (781) 830-4899 or Samantha.Vogt@massmail.state.ma.us.

- Examples of types of evidence/data can search for on digital devices with probable cause:

Text messages/chats/instant messages	Notes
Photos/videos/metadata associated	Activity Data
Contact lists/ "In Case of Emergency"	Significant or cached locations
Call Logs	Location/GPS data
Web/Search History	Applications / User Accounts
Emails	Bookmarks
Voicemails	Telephone number
Stored passcodes	IMEI/MEID/Serial number
Deleted data	Social Media Applications

- In drafting search warrant, request permission to SEIZE the entire contents of the digital device and SEARCH only for what you have probable cause for. If you are using a civilian examiner, the civilians must be written into the warrant.

    - Example: "Digital forensics is a branch of forensic science encompassing the recovery, preservation, investigation, examination, and analysis of material found on digital devices, most often mobile cellphones and computers. Digital forensic software allows forensic examiners to extract data from digital devices and parse it into a readable format. I know from my training and experience that a majority of software programs do not allow for date/time/content restrictions and require the acquisition and extraction of all data from a digital device. Because of these software limitations, I request permission to seize all data contained on _____ and with the assistance of a forensic examiner, either a civilian or police officer, search only the data authorized by this warrant.
    - If in past experience, a 3rd party provider like Google, Facebook, etc… disregarded date ranges and sent all records, include this in your affidavit and explain that the search will be limited to the parameters and timeframe provided by the warrant.

- **TIME LIMITS**
    - Temporal limits are **REQUIRED** – start and end date supported by probable cause. See Snow, 486 Mass. 582 (2021).
    - "Err on the side of narrowness" in initial SW. If additional information supports probable cause to expand the search, seek second warrant.

- **NEXUS/PARTICULARITY**
    - Specify the particular items of evidence to be searched (ex: data, including photos and videos, evidencing communications between X and Y on date and include known phone numbers, emails, usernames, etc…)
    - If you know where on a device the data could be found, must state (ex: a particular app parties used to communicate). See Snow, 486 Mass. 582 (2021); Henley, 488 Mass. 95 (2021).

- **DO NOT DELAY**
  - Once you seize a cellphone or digital device, must obtain search warrant within reasonable time. The NDAO suggests a reasonable time is less than 10 days. See White, 475 Mass. 583 (2016).

- **CONSENT**
  - Search warrants are preferred over consent. If consent is provided, obtain in writing and video/audio record.

- **PLAIN VIEW**
  - If legally in a device and see evidence beyond the scope of your current search warrant, stop search and apply for second warrant.

- **TERMS OF SERVICES**
  - Include terms and service agreements, generally available on company's website as attachments incorporated into the search warrant.
  - Request time and date user accepted applications' terms and service agreement.

- **PRESERVATION ORDERS PURSUANT 18 U.S.C. § 2703(F)**
  - Submit to company/service provider to preserve data for 90 days. Can be renewed for additional 90 days.
  - Police should file ASAP - certain apps. (ex: snapchat) destroy data in 24 hours

- **NON-DISCLOSURE ORDER PURSUANT TO 18 U.S.C. § 2705(B)**
  - Most companies notify users of law enforcement's request for legal process.
  - Requires judge's signature. Obtain separate signed court order that must accompany the search warrant being sent to the provider.

SPECIFIC DIGITAL EVIDENCE WARRANTS

- **BODY CAMERAS**
  - If seek to review body camera footage from a different incident (even if related and within the same police department) must obtain a search warrant. See Yusuf, 488 Mass. 379 (2021).
  - If seeking search warrant for a residence and your department utilizes body cameras, the NDAO suggests disclosing body cameras in the affidavit and request permission to record search.

- **CELL PHONES**
  - **MUST** demonstrate suspect actually used or possessed phone during commission of the crime (includes planning, preparation, flight).
  - Establish "specific, not speculative" evidence phone contains evidence of crime. Can be based on direct observations, nature of evidence, and normal inferences. See Henley, 488 Mass. 95 (2021); Snow, 486 Mass. 582 (2021).
  - Search warrant relying on "ubiquitous presence" of phones and text messages or generalities used to communicate are insufficient to establish nexus to search.

- **CSLI (cell site location information)**
  - Warrant provides cell provider's phone records of location data.
  - While not necessary to demonstrate suspect actually used or possessed phone during crime, must show there is a substantial basis to conclude suspect used cell phone during the relevant period, so that there is probable cause CSLI will produce evidence of crime. See Hobbs, 482 Mass. 538 (2019).
  - If investigating a pattern of activity, the NDAO suggests requesting 30 days of CSLI to show pattern, inculpatory and exculpatory information. Also may request any records of account holder complaining of unauthorized use.

- **GEOFENCE (Geographical filtered data warrants directed to Google)**
  - Provides deidentified data from Google in three phases – must seek warrant for all three. First two warrants Google may provide list of devices within specific location coordinates at specific times. The third warrant Google may provide information about the owner of the accounts associated with a device.
  - Zones should be narrowly drawn and time restricted to avoid extraneous and unrelated data points.
  - Err on side of caution and have Superior Court Judge sign warrant.
  - If include private home/area get permission from owner and include in affidavit.
  - Use sparingly – if you have a question whether appropriate please call NDAO.

- **PING WARRANTS**
  - For live GPS location of device, not for content of communications.
  - Obtain search warrant and NDAO suggests timeframe should be no longer than 15 days. Can always seek second warrant. See Almonor, 482 Mass. 35 (2019).
  - Absent exigent circumstances, call NDAO before requesting a ping warrant.

- **POLE CAMERAS**
  - Must obtain search warrant before installing pole camera aimed at a residence. See Mora, 485 Mass. 360 (2020); Comenzo, 489 Mass. 155 (2022).
  - Establish probable cause camera will capture evidence of a crime or will aide in establishing the identity or apprehension of an individual that you have probable cause to believe committed a crime.
  - Must include narrow timeframe for how long camera will be installed.

- **TOWER DUMPS**
  - Search warrant MUST include "protocols for the prompt and permanent disposal of any and all data that does not fit within the object of the search following the conclusion of the prosecution." Do not destroy data until speaking with NDAO.
  - Explain request is to compare different zones to determine common telephone numbers that could "identify and/or verify commonalities within the requested records for the purposes of identifying a common suspect." See Perry, 489 Mass. 436 (2022).
  - Judge MUST issue search warrant.



TAILORED. VIDEO. INTELLIGENCE.

AIRSHIP NEXUS MOBILE APP

QUICK REFERENCE GUIDE

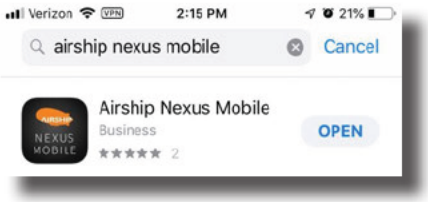
CONTENTS

ABOUT AIRSHIP NEXUS MOBILE 3
Select or Add a Server to Log In 3
MAIN SCREEN FEATURES 4
Assets Menu 4
GLOBAL ACTIONS MENU 5
Settings Menu 5
Views List 6
Main Screen Gestures 6
Hosted Clips 6
SINGLE SCREEN FEATURES 7
Live View 7
Playback 7
LANDSCAPE MODE 8

ABOUT AIRSHIP NEXUS MOBILE

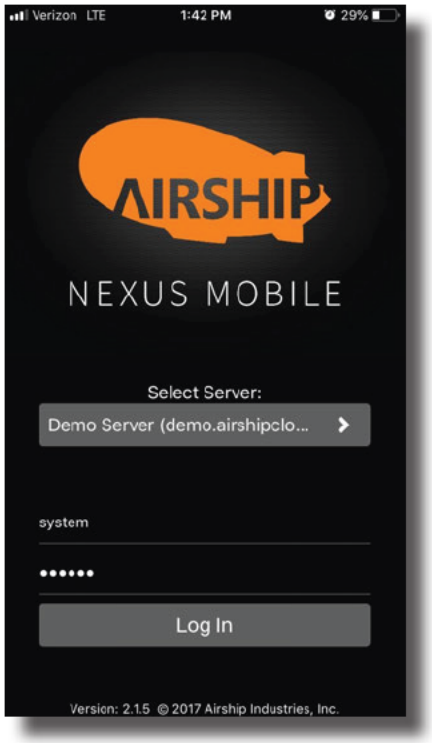
Nexus Mobile is the mobile app for viewing video over **Airship VMS**. **Nexus Mobile's** extensive features are designed to work exclusively with **Airship VMS**, and **Nexus Mobile** ***must be connected*** to a VMS ("server") to operate.

Before beginning, visit the App store or Google Play store to download **Airship Nexus Mobile**.



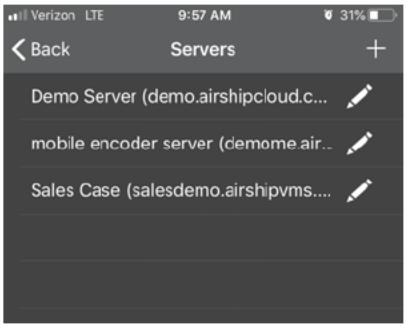
Select or Add a Server to Log In

A login screen appears after launching the app with a **Select Server** button. Before logging in, select a **Nexus Video Portal** server to connect to, or add a new server by its IP or hostname.



Tap the **Select Server** button to go to the server list. If the desired server has already been added, simply tap it and proceed with to login using the appropriate username and password. Otherwise, follow the instructions below to add a new server:

1. Tap the **plus sign (+)** in the upper right corner to ***add a server***.



2. Enter a name for the Server, the IP address and port of the Server that will be connected. Click the SSL toggle switch on (green) if using SSL.

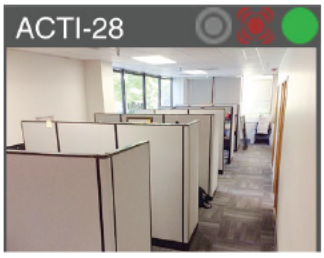
> 🕮 **NOTE:** Contact the system administrator if specific IP and Port information is unknown.

3. When finished, tap **Done** in the upper-right corner to return to the server list.
4. The new server will appear in the server list under "Select Server." Select the newly added Server, type in the appropriate credentials, then click **Log In**.



MAIN SCREEN FEATURES

Nexus Mobile's main screen **displays six channels at once**. Users can view cameras live and in playback. Each viewport has the following status indicators above its viewing pane:



Recording Status:

- Recording Off
- Recording Video Only
- Recording Audio & Video

Alarm Status:

- Alarm Off
- Alarm On
- Alarm Triggered

Connection Status:

- Disconnected
- Live View Mode
- Playback Mode

There are **three main screen menus** from which to access configuration and viewing settings**.** Tap the icons in the corners of the screen to access these menus. The following sections will cover the available settings available to each menu.

Assets	Select devices to display in the viewing grid.
Global Actions	Select from common actions, such as changing Settings, disconnecting all cameras, or logging out.
Views List	Create and launch custom viewing grid views

Assets Menu

①**Search**: Enter the first letters of the device you wish to find.

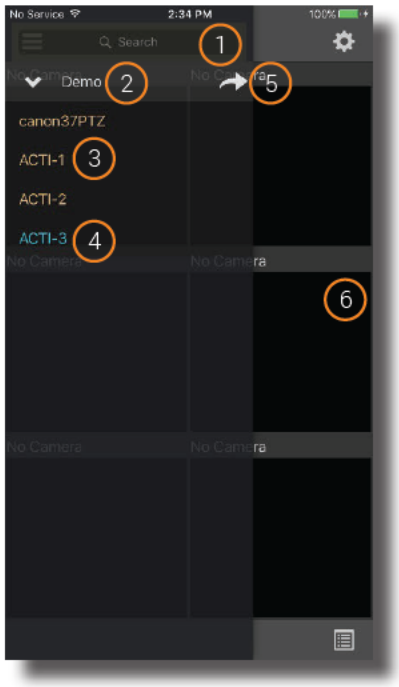
②**Server**: Displays the name of the server. Expands to show server (s) cameras.

③**Individual Camera**: Tap any camera here to add it to the grid.

④**Camera in Playback Mode**: Name displayed in blue.

⑤**Connect All**: Tap this arrow to connect and display all cameras in the group in the main viewing grid.

⑥**Main Viewing Grid**: Tap here (outside the Assets List) to close the list.



GLOBAL ACTIONS MENU

①**Global Actions Menu :** Tap here to open the global actions menu.

②**Hosted Clips:** Tap to view list of Hosted Clips.

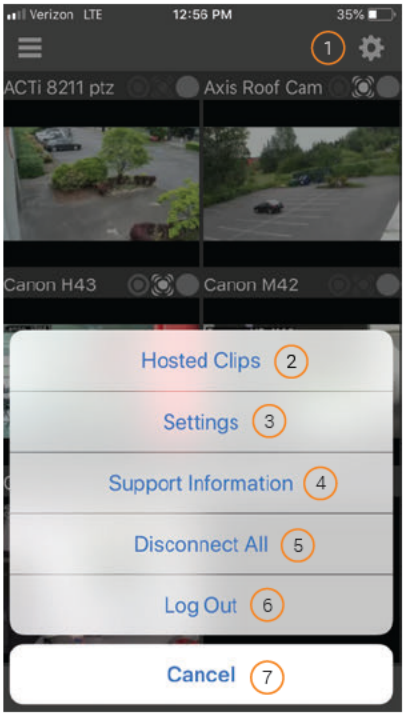
③**Settings:** Goes to settings screen to select options such as Touch ID, H264, and Camera Timeout.

④**Support Information**: Get information about Airship Support.

⑤**Disconnect All:** Disconnect all cameras in the camera grid.

⑥**Log Out**: Log out of the current session and go back to the login screen.

⑦**Cancel**: Close this menu.



Settings Menu

①**Back** Save settings and return to the main screen.

②**Use H264:** Enable the use of the H264 encode type (recommended to enable).

③**Use Local Time** Use the time local to the mobile device instead of the server's time.

④**Camera Timeout**: The amount of time the app attempts to connect to the camera before shutting down the connection.

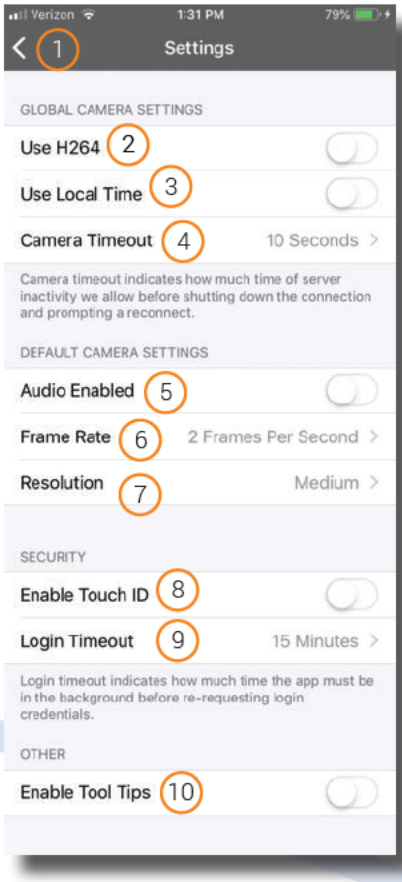
⑤**Audio Enabled** While enabled, audio will be on by default for all audio-capable channels.

⑥**Frame Rate:** Sets the streaming frame rate.

⑦**Resolution:** Select the streaming resolution that best suits the network connection.

⑧**Enable Touch ID or Face ID:** Enable/Disables Touch or Face ID login as a feature based on which feature is available for the mobile device.

📖 Touch or Face ID must be set up on the device prior to enabling the feature. The login credentials used to enable Touch or Face ID will be automatically entered upon next login.



⑨**Login Timeout** Amount of time until app logs out while running in the background or when not in use.

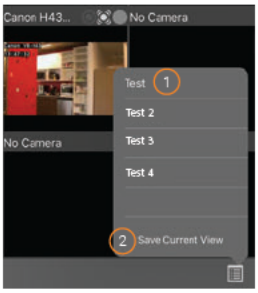
⑩**Enable Tool Tips:** Toggle tooltips for new users. These will automatically show for the first use of the tool, then shut off.

Views List

Once the main viewing grid has all the desired cameras in the desired viewports, **users can save views** to be recalled at a later time.

①**View Name:** Tap on a view's name to "call" it, then it will populate on the main viewing grid.

②**Save Current:** To save a new view, place all cameras in the desired viewports in the desired order, type in the name of the new view, and then click the **Save Current** button. The new view will be added to the list with its new name.



Main Screen Gestures

Several gestures are available to the user for control of various parts of the app:

Snapshot: Double-tap on a viewport to take a snapshot of that camera's current view.

Single-View: Single-tap on a viewport to show that camera in single-view

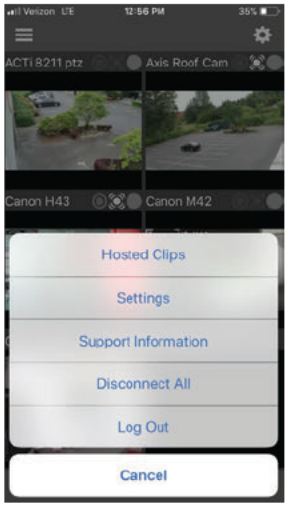
Swappable Viewports: Move a viewport to a different slot by holding and dragging it to that desired slot and dropping it. This will cause the two viewports to switch places.

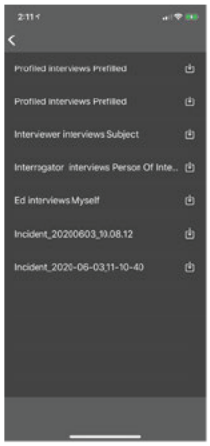
Camera Disconnect: Drag a viewport off the screen to disconnect its associated camera.

Hosted Clips

Hosted clips are available for playback on **Nexus Video Portal** and locally on **Nexus Mobile**. To access available clips from Nexus Mobile, click the Global Actions gear icon in the top right corner while viewing multiple cameras, and select **Hosted Clips**.

Click on an incident fron the list of hosted clips to view and playback will begin. Click on the download icon next to the clip in order to save footage to the native camera roll.

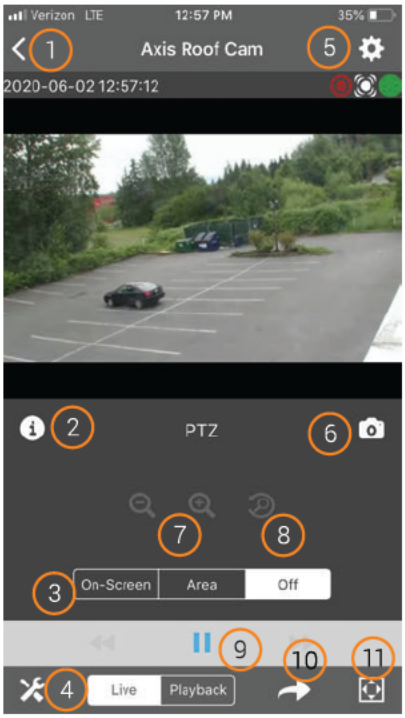




SINGLE SCREEN FEATURES

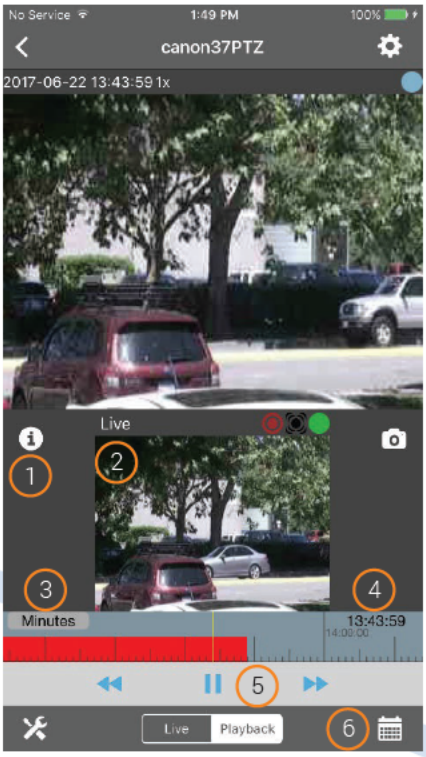
The single-screen view provides several features, options, and controls for a single camera that are not available from the main grid view. Some controls will change between live and playback.

Live View



①**Back**:	Return to the main grid view.
②**PTZ Help**:	Get helpful information about the different PTZ modes.
③**PTZ Mode**:	Choose the desired PTZ mode.
④**Video Settings**:	Adjust settings such as frame rate and resolution.
⑤**Global Actions:**	Open the global quick action menu.
⑥**Snapshot:**	Take a still shot of the camera's current view.
⑦**Zoom In/Out**:	Zoom any PTZ-capable camera in and out with these controls.
⑧**Reset Zoom:**	If zoomed in, tap here to zoom the camera all the way out.
⑨**Camera State**:	Choose whether to view live or playback video.
⑩ **Export Clip**	Tap to view Export options, which saves to Hosted Clips.
⑪ **PTZ Presets**:	Save and call presets from this list.

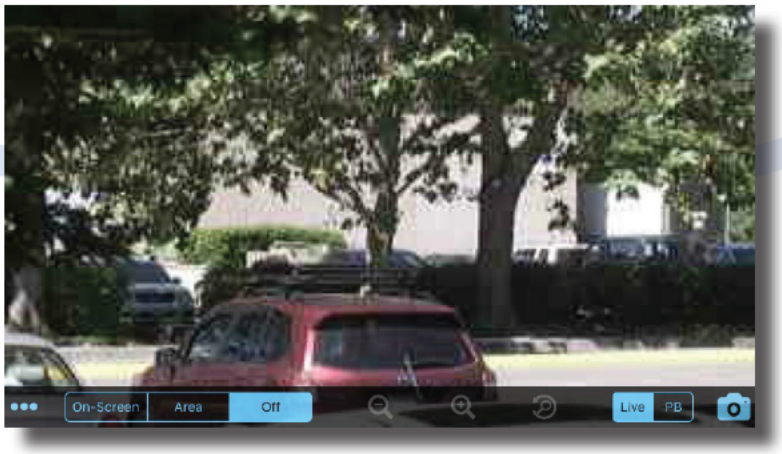
Playback



①**Timeline Help**:	Get helpful information about the various controls available for the timeline.
②**Picture-in-picture**:	Get the live stream along with the playback video.
③**Timeline Scale**:	Choose between hours, minutes, and seconds.
④**Timeline:**	See and control where in time the video is playing.
⑤**Playback Controls**:	Rewind, Play/Pause and Fast Forward the video as needed.
⑥**Calendar**:	Select the date from which to view footage.

LANDSCAPE MODE

Nexus Mobile also supports the **Landscape** orientation on certain screens. As landscape is intended to give the maximum viewing area possible, not all the same functionality will be available while in landscape, but the core features will be highlighted.



[end]
rev:202006171029



TAILORED. VIDEO. INTELLIGENCE.

NEXUS CLIENT

USER MANUAL

TABLE OF CONTENTS

COPYRIGHT AND DISCLAIMER 5
Copyright 5
Disclaimer 5
Target Audience 5
LAUNCH NEXUS CLIENT 6
Log in to Nexus 6
NEXUS CLIENT MAIN WINDOW 7
Working with Tab Basics 7
Creating a New Tab 7
Deleting a Tab: 8
Tab Tear Off 8
Toggling Between a Torn Off Tab 9
Favorite Tabs 9
SERVER MANAGEMENT 10
Configure a Server 11
VIEWING LIVE VIDEO 12
Adding Cameras to the Screen 12
Assets 12
Add Bookmark 13
Viewing Modes 14
Video Toolbar 15
Views 15
Video 15
Info 15
Exporting and Bookmarking 16
PTZ Controls 16
On-Screen PTZ 18
Snapshot Viewer 20
Lock Clip 21
High Resolution Download Feature 22
Rimage Publisher 23
CREATING CUSTOM VIEWS 24
Using the Video Tab 24
Creating a View in the Video Tab: 24
Toolbar Options 24
Toolbar Options 25
Views 26
Web Page 26
Video Content 26
SAVING DEWARPED VIEWS 27
SEARCH FOR RECORDED VIDEO 28
Using the Weekly Search Tab 28
Toolbar Options 29
Assets 29

©2021 Airship Industries

Calendar *30*
Using the Video tab 30
Timeline Tools *30*
ALARM CONSOLE 32
Toolbar Options 33
Alarm Filter Options *34*
LICENSE PLATE SEARCH 35
FACIAL RECOGNITION 35
MAPS 36
E-Maps 36
Live Map 37
Use Setup Wizard to Orient Cameras/Devices *38*
Edit Mode Enabled *39*
THUMBNAIL SEARCH 40
TRACKDATA 41
Toolbar Options 41
WALL DESIGNER 42
Wall Driver 42
Add a Driver *42*
Toolbar Options 43
Current Monitor 44
Right-click Options *44*
Monitors 44
Right-click Options *44*
Salvos/Views 45
Right-click Options *45*
Current Video Wall 45
Activity Log *45*
WALL CONTROLLER 46
Toolbar Options 46
Current Monitor 46
Right-click Options *46*
Current Video Wall *46*
NEXUS CLIENT OPTIONS 47
Video Options 47
Alarms 49
Export 50
Save/Load Windows 51
OSD 51
Mapping 52
Map Layers 53
License Plate Options 54
Rimage Publisher 54
Managed Mode 55
Adding a New EMS *56*

Modify an Existing EMS *57*
Nexus Client License 57
Filters 59
Serial Information 59
Misc 60
Snapshot *60*
Joystick *60*
Alias *60*
Emap *60*
Backup/Restore 61
PTZ 61
About 61
Advanced 62
Configure Server Settings through Nexus Client 62
General 63
Startup and Exit *63*
Alarm *63*
Video Storage *63*
Miscellaneous Options *65*
Network 65
Remote Client Service *65*
SSL Settings *66*
E-mail *66*
Devices 67
Add a Camera *67*
Configure a Camera *67*
Add Multiple Cameras *69*
Cameras 70
Display *70*
Color *71*
Video and Schedule *72*
PTZ *72*
Alarms *73*
Motion Area *74*
NEXUS VERSION HISTORY 76

©2021 Airship Industries

COPYRIGHT AND DISCLAIMER

Copyright

This publication, including all photographs, illustrations, instructions, and software, is the property of Airship Industries, Inc. The copyrights and intellectual property rights associated with this publication and its contents are protected by international copyright laws, with all rights reserved. Neither this manual nor any of the material contained herein, may be rewritten, reproduced or shown to the public without first receiving the written consent of Airship.

Disclaimer

The information in this document has been prepared by Airship's current system policies and procedures and is subject to change without notice. Airship reserves the right to revise or amend this publication and make changes periodically, without any obligation to notify any person of such amendments or revisions.

Airship makes no representations or warranties that the hardware will work properly in all environments and applications, and specifically disclaims any implied or express warranties with regard to the quality, performance, merchantability, or fitness for a particular purpose.

In no event shall the copyright owner or contributors to this manual be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including but not limited to procurement of substitute goods or services, loss of use, data, or profits, or business opportunity), however caused and arising out of any theory of recovery, arising out of the use of this software.

Target Audience

This manual is intended for end users of **Airship Nexus Client Video Management Software**. This manual provides a detailed description of viewing live video and playback using different tabs in **Nexus Client**.

Contact your system administrator if you have questions on your individual or agency's setup prior to making changes in **Nexus Client**, as certain could impact your user experience.

LAUNCH NEXUS CLIENT

Log in to Nexus

To begin, double-click the **Launch Nexus Client** icon to open the application. Nexus launches a **Log in to Nexus Client** dialog box. Input the username and password.



Name: Enter a username.

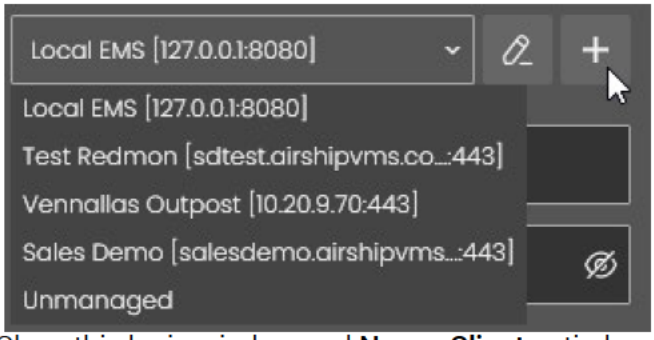
Password: Enter a password.

Log in: Click the Log in button to log into **Nexus Client** using the entered username and password.

📖 **HELPFUL HINTS:** Single Sign-On (SSO) allows a user to log in to **Nexus Client** using their Windows domain credentials. Setup is required to enable this feature. See ***Airship's SSO Quick Reference Guide*** for more information.

Log in Automatically: Select this checkbox to save the currently used login method (either username and password or SSO) for future use. The next time **Nexus Client** is launched, it opens directly to the **Video** tab without first showing the login window.

EMS Dropdown: If an **EMS** has already been added, select the desired **EMS** here. If not, click the dropdown and select the **+** button to add the new **EMS**'s info in the popup that appears. If no **EMS** is desired, select **Unmanaged**.



Exit Client: Close this login window and **Nexus Client** entirely.

Users can also add an **EMS** to their **Nexus Client** under Options > Managed Mode. While logging into Nexus, users can select the **EMS** from the dropdown selection as shown in the screenshot above.

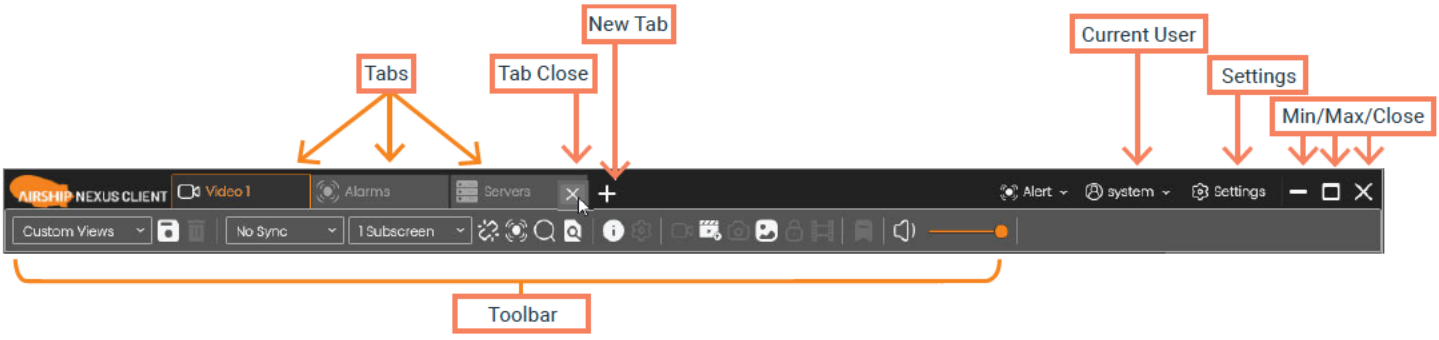
©2021 Airship Industries

NEXUS CLIENT MAIN WINDOW

Nexus Client lets users pull live and recorded video from a multitude of Airship DVRs/NVRs and interact with that video in a simple and intuitive way. With **Nexus Client**, users view real-time camera footage, as well as previously recorded footage in the default screen configurations or in custom-designed views.

Users can save video clips as self-executable files ("EXE") or mp4 files to play the recordings on other machines, or take snapshots of live and recorded video.

If users have more than one physical display attached, they can send individual views to separate windows, and watch more than one view at a time.



Working with Tab Basics

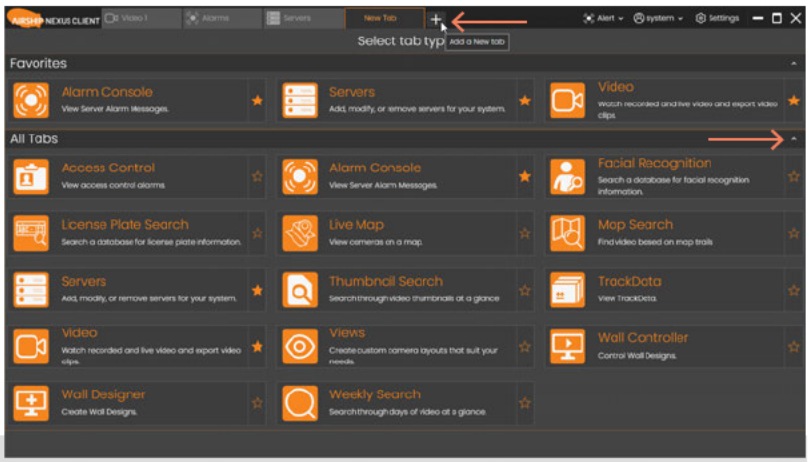
Nexus Client allows the user to create multiple tabs much like a web browser to keep multiple tools (e.g. Video, Search, Map) readily available within a single window. In addition, these tabs can be torn off from their current window to create a whole new window, allowing you to optimize your workspace.

Creating a New Tab

Follow the steps below to create a new tab:

1. Click the + icon to create a new tab.
2. Select the type of tab desired. Favorites will appear at the top. To view All Tabs, click the drop-down arrow to the right of the menu screen.
3. Click on the desired page icon to open that page as a new tab.

   The user can move tabs within the main window to suit their needs or remove them to create a new window.



📖 **Helpful Hint:** The Servers tab will only permit one instance to be open at a time.

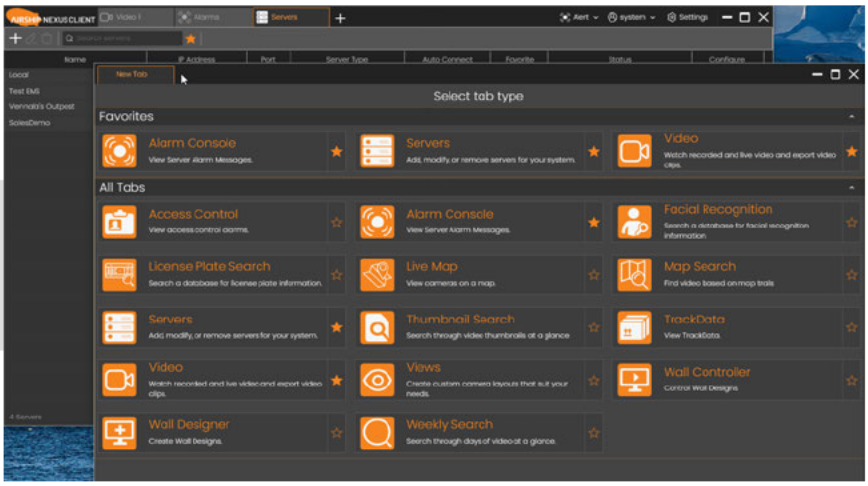
Deleting a Tab:

The user can remove the tabs, except for the **original Video tab**. Go to the tab and click the button at the end or middle-click on the mouse to close or remove the tab.

Tab Tear Off

Users can tear a tab off **Nexus Client** in order to view multiple screens at one time. The following steps show the user how to **tear a tab off for video**.

1. Click the icon near the top of the toolbar to create a new tab.
2. Select video option in the newly opened tab.



> 🕮 **IMPORTANT:** Only *video tear off tabs* can be toggled through. Other tab types can be torn off, but the user will not be able to maneuver through them.

3. Once the new video tab is successfully opened, hover the mouse over the new tab, click the desired option, and drag the tab off away from the **Nexus Client** window. See above.
4. At this point, the user can place screens in the desired manner.

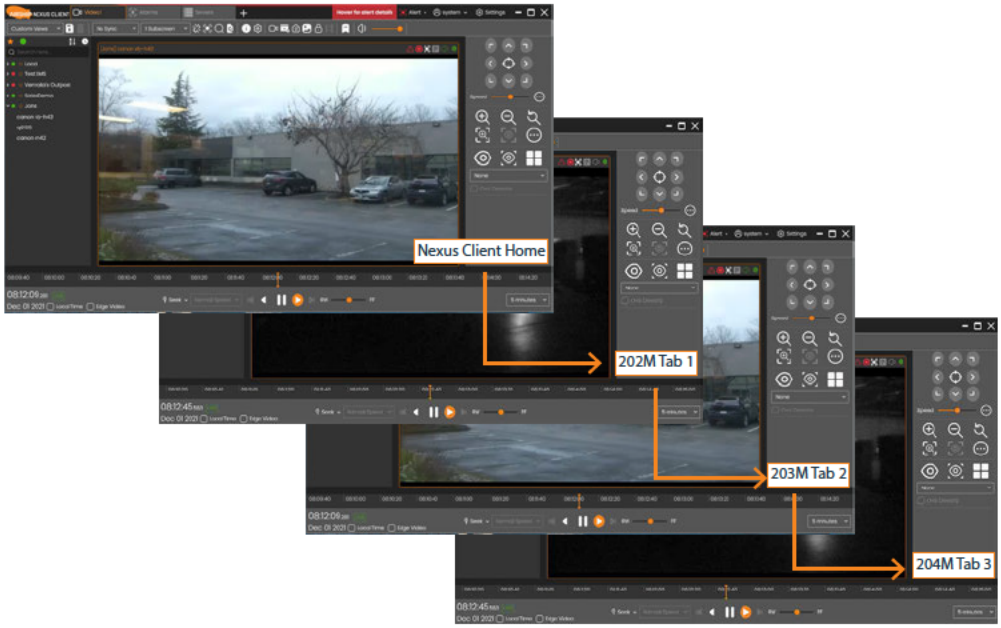
> 🕮 **IMPORTANT:** Users can ***only*** tear off tabs from the main **Nexus Client** screen. Tabs which are torn off can rejoin the main client window by clicking and dragging tabs next to each other.

©2021 Airship Industries

Toggling Between a Torn Off Tab

Users also have the option to **toggle back and forth between torn off video tabs** with specific keyboard shortcuts. The following steps show users how to maneuver through **torn off video tabs**.

1. Users can toggle between windows by using the key command, "**#M**." The **#** symbol represents the tab number, while the **M** is inputted ***after*** the tab number. d
2. Typing **201M** will bring the user back to the **Nexus Client home screen**.
   Typing **202M** will move the user to the first torn off tab; Typing **203M** will move the user to the second torn off tab; Typing **204M** will move the user to the third torn off tab; and so on.

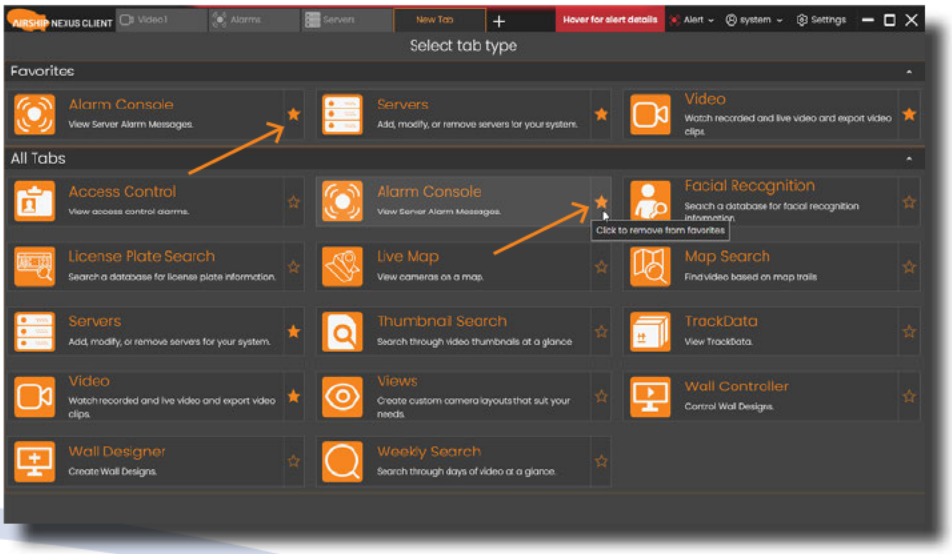


For example, if a user has the main **Nexus Client** screen and three tear away tabs open, the screens would be named by **order of opening the tabs**. Simply type the desired keyboard command to sift through screens. ***See right.***

> 🕮 **IMPORTANT:** Users need to have **Nexus Client** highlighted (i.e., clicked on/engaged) to toggle between screens, or, users may open other desktop programs. If another program is running, such as Google Chrome, pressing the key commands may open up certain Google Chrome features.

Favorite Tabs

For quick access to your most commonly used tabs, click the star next to tab name (show below). The tab will sort to the top of the **Favorites** section. There is no limit to the number of favorites chosen.



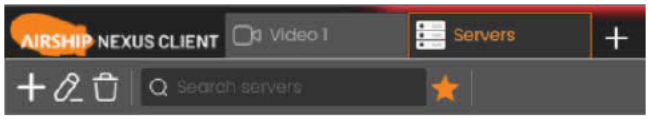
SERVER MANAGEMENT

The **Servers** tab will allow the user to add new servers by providing the IP address and Port number. A user can view the list of all servers along with their connection status in this tab. A user with valid permission can access each Server's settings from **Nexus Client.**

By default, the username/password used to log in to **Nexus Client** will be used to connect to each of the servers in the list. If a particular server requires a different username and password, the user can change it in the **Log in with specific user** option. The **Server Management** toolbar also provides options to edit or delete the existing servers.

> 🕮 **IMPORTANT:** *Users cannot add, edit, or delete a server when* **Nexus Client** *while in managed mode. See* "Managed Mode" covered on page 55.

Add: Click the **Add** button to add a new server.



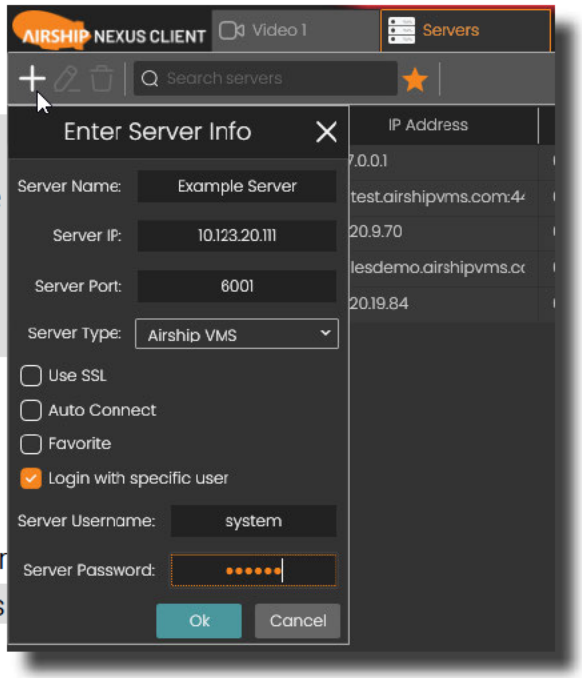
Edit: Select a server in the list and click the **Edit** button to modify the server information. The selected server is highlighted in yellow.

Delete: Select a server and click the **Delete** button to remove the server.

> 🕮 **HELPFUL HINTS:** In **Nexus Client**, users in Managed Mode cannot see the **Servers** toolbar. They only see the list of servers they have been granted access to through the **EMS**.

Follow the steps below to add a new DVR/server.

1. Open the **Servers** tab if it already exists or click the ⊞ button at the top of the main window to open a new tab and select the **Servers** page type.
2. Click the **Add** button from the **Server Management** Toolbar to add a new row as shown in the screenshot above. The default name is set as "New Server".
3. Enter the server information as directed by the open fields (outlined below) to add a new server.



> 🕮 Checking the box labeled **Log in with specific user** will automatically use the credentials provided to connect and authenticate access. You must double click the Server line for these options to appear.
> If the **Log in with specific user** option is unchecked, by default, the current user's username and password will be used to connect to the selected Server.

Enter or select the appropriate information:

Name: Enter a name for the server.

IP Address: Enter the IP address of the server

Port: Enter the Port number for the server

> 🕮 **Helpful Hint:** The default port is

©2021 Airship Industries

Category: Airship DVR/NVR; Airship Embedded, Nexus VMS, Hanwha NVR or Webgate VMS.

📖 **New Feature:** For Hanwha NVR or Webgate VMS, enter the IP address or hostname to connect to existing NVR/DVRs. If **EMS** is managing Airship Servers, simply add the NVR/DVR from the Servers page in **EMS**. See the ***Airship EMS System Adminstrator QRG*** for more information on adding Servers.

Use SSL: Select this option if you want to use SSL.

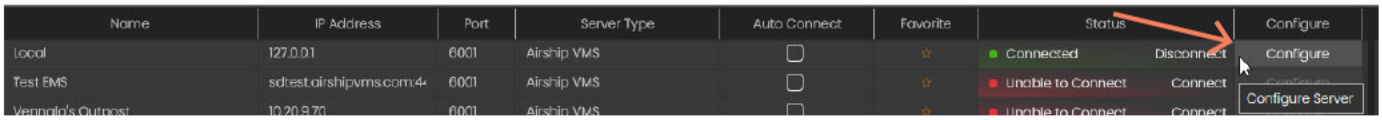
Favorite: Click this box to add as a **Favorite** server.

Auto-Connect: When a user logs in to **Nexus Client**, the **Auto-Connect** option will enable a connection to the server automatically. Enabling this option will also reconnect to the server if a server connection is lost for any reason.

Status: The **Status** column displays the connection state of the listed server(s). A green dot indicates a "Connected" status. A red dot indicates an **"**Unable to Connect" status. The user can connect/disconnect to a server manually using the connect/disconnect buttons for each server based on its current status.

Configure a Server

A user with valid username and password can access each server's settings by clicking the **Configure** button. Click **Configure** to display the network and system settings for the server selected.



📖 **IMPORTANT:** Server configuration options may be restricted depending the user's permission settings in the **EMS**. The **"**Configure" option is only available when a Server status is 'connected'.

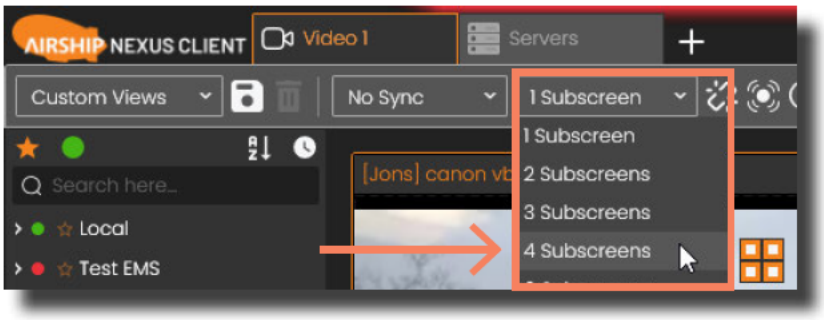
Refer to "Configure Server Settings through Nexus Client" covered on page 61 to learn more about server configurations within **Nexus Client**.

VIEWING LIVE VIDEO

The **Video** tab is used to display video in Live and Playback. A user can view all the footage from various cameras displayed in the center part of the window, which is called the **screen.**

Adding Cameras to the Screen

Follow the steps below to add cameras:



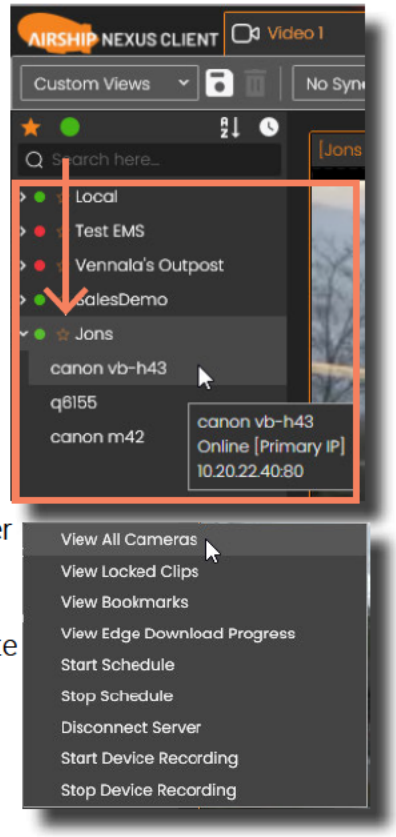
1. Open the **Video** tab and select a Server from under the **Assets** list, this expands the camera list to choose a Camera. Refer to the Assets section for more information.
2. Add subscreens to the screen by choosing the number of subscreens from the video toolbar.
3. Using the mouse, select a camera from the **Assets** panel and drag it on to a subscreen to view the video from that camera.
4. You can add up to 36 subscreens at a time.

> 🕮 **HELPFUL HINTS:** The default value for the maximum number of screens is "No Limit" which you can change under Options > Video Options.

Users can quickly switch a camera from Live to Playback without removing the camera from the subscreen. When a user has more than one subscreen, a camera can be moved from one subscreen to other. The existing camera on that subscreen will be replaced by the new camera.

Assets

The **Assets** panel displays all available servers and cameras to the **Nexus Client** as shown in the screenshot on the right. Click on the arrow next to a server's name to see the cameras added to that server. The list of cameras and servers is updated when you log out and back in to Nexus Client. The selected camera's name is highlighted to the left of the name.

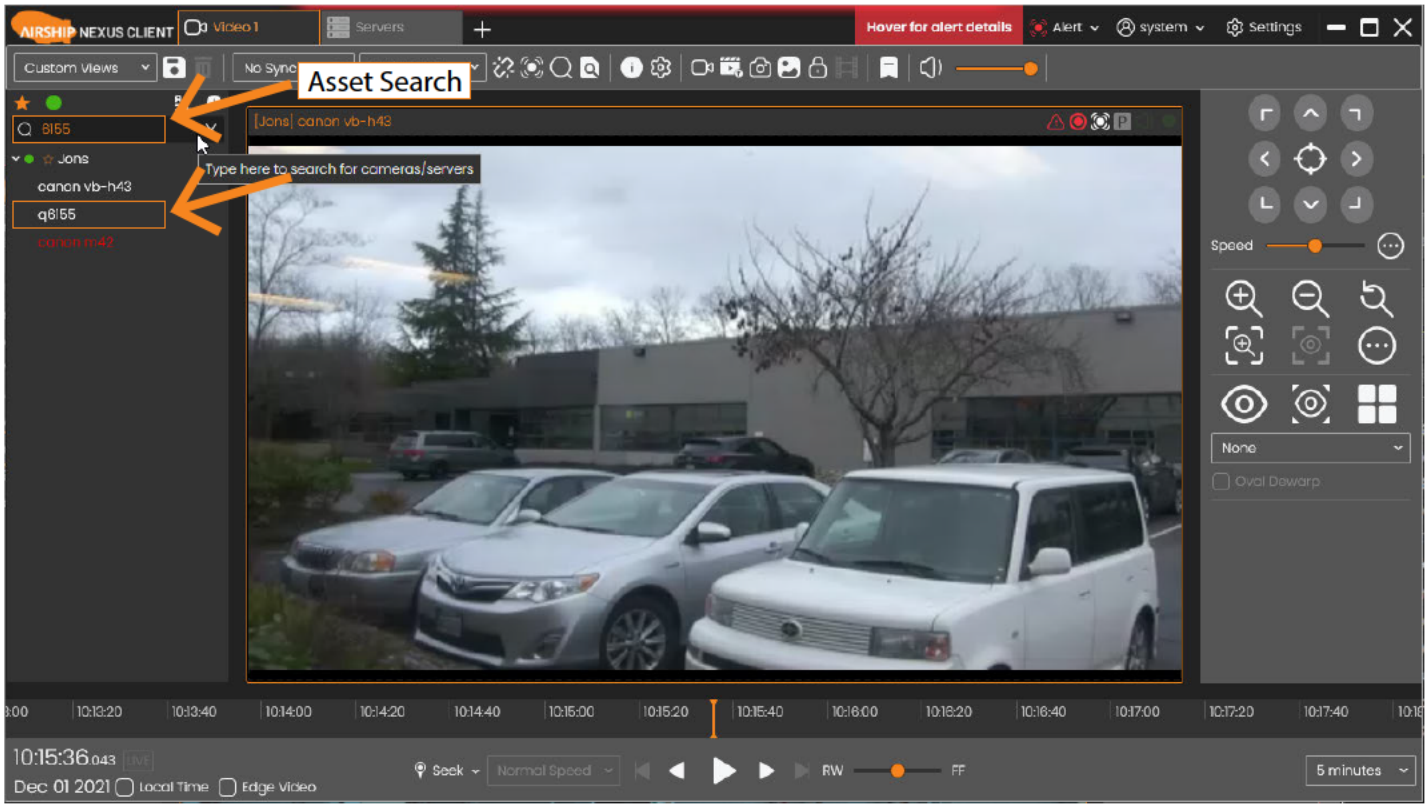


1. Right-click on a Server, VSH, Case or Outpost to select from the option seen on the right.
2. Clicking **View All Cameras** will display all connected devices for that Server or Outpost.
3. Locked Clips and Bookmarks associated with the selected Server can be viewed quickly, as well as Edge Downloads can be downloaded from remote Outpost devices for high-quality review.
4. Schedules may be started or stopped per Server this way as well.
5. Additionally, you may disconnect your connection to the Server, or add it to Favorites for quick access using this right-click selection.

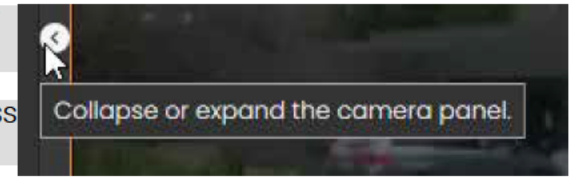
©2021 Airship Industries

Asset Search

Asset Search displays the list of all connected cameras and servers. Search for a particular camera or server by entering its name in the search box.



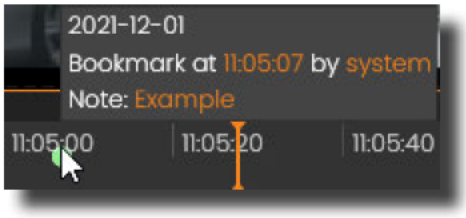
📖 **HELPFUL HINTS**: Collapse or expand the video screen by hovering over the edges of the video screen and clicking.



📖 **HELPFUL HINTS:** To enter and exit full screen mode, press the escape key.

Add Bookmark

Bookmarks allow the user to quickly enter playback at a specified time. To add a bookmark, navigate to the time where you would like playback footage to begin, click "Add Bookmark", and add a note for reference once prompted.

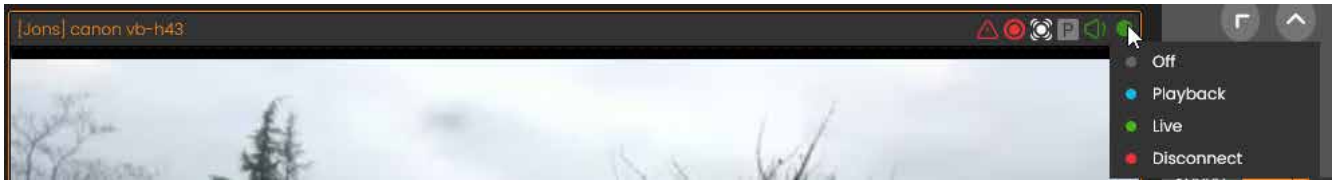


Hovering over a bookmark with the mouse will display the note added.

Viewing Modes

At the top of each subscreen are icons which indicate various states for that camera. These icons are (from left to right): recording state, alarm state, presets, and camera mode.

There are four modes for each camera: Off, Playback, Live and Disconnect. The **Off** button will turn the camera's display off in its subscreen. The **Playback** button will show that camera's previously recorded footage. The **Live** button will display the current video of that camera. The **Disconnect** button will stop the video for that camera and will completely remove it from its subscreen.



Channel Capacity: An icon is displayed during Live video streaming if the storage capacity is full.

Storage capacity full

Video Integrity: Airship Server automatically checks video integrity (if enabled on Server) for each channel when in playback mode. Server sends this information to **Nexus Client**, and this icon simply indicates the result of that check.

Video integrity uncertain

Video integrity secure

Video integrity compromised

Select Recording State: Click the first button to see the state of the recording.

To toggle between states, refer to "Video and Schedule" covered on page 71.

Record Off

Record video only

Record audio and video

Select Alarm State: Click the second button to see the state of the alarm.

Alarm is OFF

Alarm is ON

Alarm triggered

Presets: Using this option, a user can select a previously assigned preset on PTZ-compatible cameras.

Call Presets

Sound:

Recieving audio frames

Muted

Receiving no audio frames

©2021 Airship Industries

Video Toolbar



Views

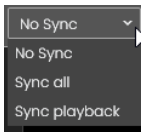


Custom Views: Saved views will appear in a drop-down list for selection.

Save View: Click to save the current view for future viewing.

Delete View: Saved views may be deleted by selecting the desired view, then click **Delete View**.

Video



No Sync: Select to independently control playback and live screens.

Sync All: Select a camera on one of the subscreens, select playback, or disconnect, and then click the **Sync All** button. All cameras on other subscreens will change to the same mode as the one just selected. In addition, all subscreens will attempt to seek to the same time and date of the selected camera.

> 🕮 **NOTE**: **Disconnect** and **Off** affect only the channel selected. To disconnect all channels, click the **Disconnect All** button.

Sync Playback: This is same as **Sync All** but applies only to the subscreens that are in playback. Subscreens in live mode do not change to playback. Clicking this will cause all cameras in playback to seek to the same time.

Disconnect All: Click the **Disconnect All** button to close all camera feeds on the current view.

Subscreens: Select the video grid desired from the subscreen list available. Refer to "Salvos/Views" covered on page 45 for more information.

Alarm Only: Select a camera in playback mode and click the **Alarm Only** button to view the triggered alarms on that camera.

Search: The **Search** button will quickly take you to the Search tab with the current cameras open for viewing. You can see the playback for those cameras in a weekly report.

Thumbnail Search: This shortcut directs to the Thumbnail Search tab, displaying the currently selected camera's playback video across thumbnails.

Info

Video Info: Select a camera on one of the subscreens and click the **Video Info** button to see all the information of that camera. A user can see server details, camera name, video codec, frame rate, bit rate, the oldest recording date, and audio details in a new window.

Configure: Click the **Configure** button to view and manage advanced video, audio, and image parameters (IP Devices only) for the currently selected camera.

Export See "Exporting a Clip" covered on page 19.

Open Clip Exports Window: Click to view the list of clip exports produced from Nexus Client.

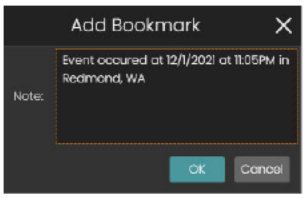
Snapshot: Saves an image of the selected video at the current time.

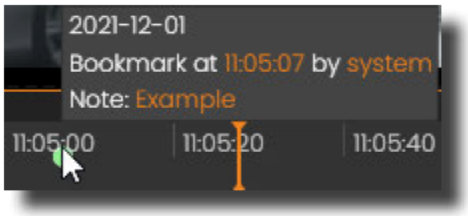
View Snapshots: Views the snapshots taken from Nexus Client.

Lock Clip: Click to create special permissions to access a particular clip. This feature is covered "Lock Clip" covered on page 21.

High Res Segment: See "High Resolution Download Feature" covered on page 22. This feature is available to Outpost devices transcoding.

Bookmarking: Click the Add Bookmark button to add a placeholder at a specific time on the timeline. A note box will pop up, which permits the user to describe a particular event.



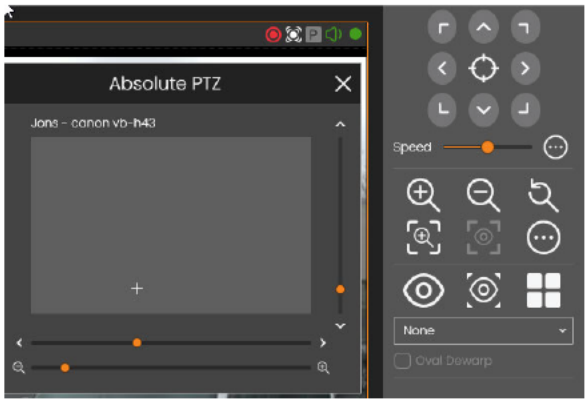


Sound Settings: Adjust the audio level for all streaming audio.

PTZ Controls

Users can find the PTZ controls at the right side of the **Video** tab. PTZ cameras are capable of remote direction and zoom control. These PTZ cameras can move their lenses horizontally (pan), vertically (tilt), as well as change their focal lengths between near and far (zoom in/zoom out).

Zoom In/Zoom Out: The **Zoom in** and **Zoom out** allows a user to see specific areas of the camera's view more clearly and get a bigger picture of what is going on in an area.



Reset Zoom: Click the **Reset Zoom** button to zoom the camera's view all the way out.

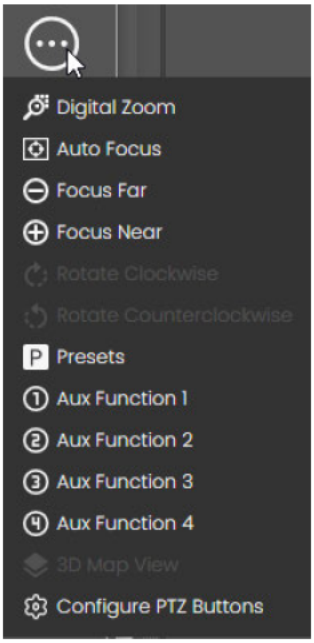
©2021 Airship Industries

On Screen PTZ: To use the Absolute PTZ Canvas, click the center button in the middle of the directional buttons. A pop-up window will appear in the center of the screen. The feature window can be dragged around.

- Clicking anywhere on a slider moves the camera's pan/tilt/zoom to that position.
- Dragging the canvas crosshair moves the camera pan and tilt.
- Double-clicking on the canvas moves the crosshair to that position and moves the camera pan and tilt.

Area of Interest: Cameras with Area of Interest options available will prioritize stream quality within the selected area. Without an area of interest area set, the full image will be prioritized equally.

Additional Options: Additional PTZ options are available by clicking the three dots.



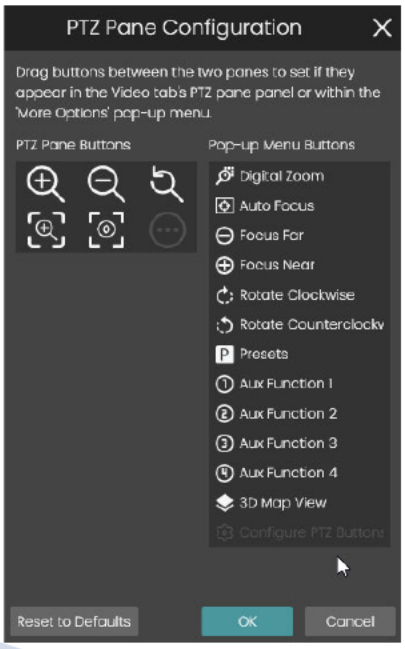
Digital Zoom is a great way to zoom into a specified portion of the screen. Draw a box around the object or area you would like to view, and the camera will Pan, Tilt, and Zoom to best represent the box drawn.

Auto-Focus automatically adjusts a camera's focus based on its proximity to objects.

Focus Far & **Focus Near** adjust the depth of focus for the selected camera.

Clockwise rotation options are available to cameras with the available capability.

The **Presets** button will open a new window with a list of previously created presets. Here you can create new presets, call presets, or delete unwanted presets. When a preset is created, the orientation of the camera will be saved either on the camera or on the server for later recall. This means presets for a given camera can be accessed in **Nexus Client** as well as in other Airship products.



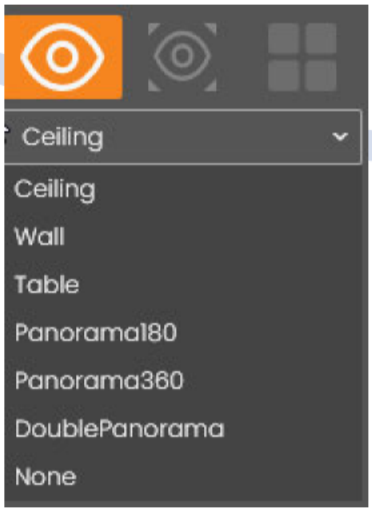
Programmed **Auxilliary PTZ Functions** may be performed by clicking one of the presets.

3D Map View options are presented when maps have been added in Settings.

Select which buttons appear on the PTZ panel by clicking **Configure PTZ buttons** (see image on right).

📖 **IMPORTANT:** All cameras might not support PTZ, Area Zoom, Presets, and Focus. Refer to the camera manufacturer's user guide for more information.

Enable dewarp view for all cameras: Clicking this icon applies fisheye Dewarp settings to the selected camera. Clcik the drop-down menu to reveal additional dewarp options.



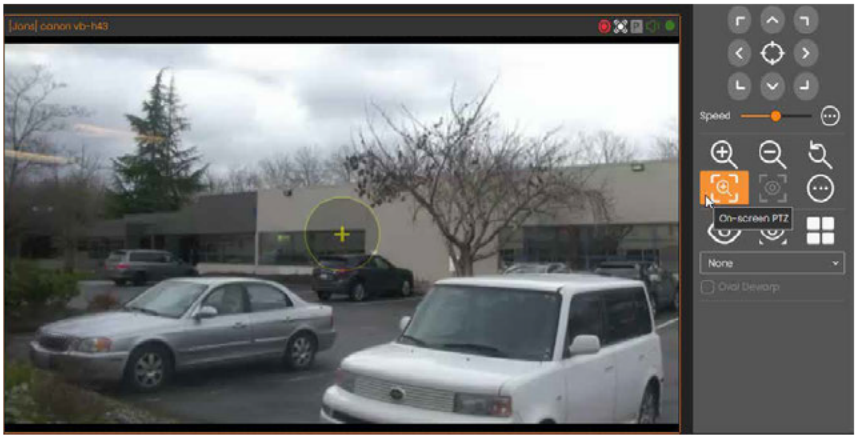
Area Dewarp: To dewarp a specific area on screen, click Area dewarp, the draw a box over the desired area. The area selected will be presented a separate dewarped screen.

Quad Dewarp: Views selected camera as 4 individually dewarped screens.

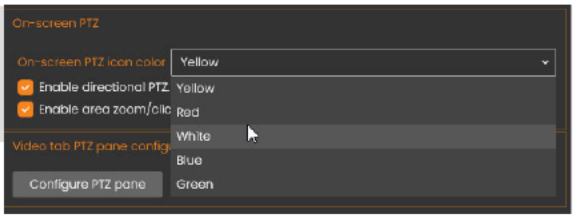
On-Screen PTZ

Toggle the on-screen PTZ by clicking the button in the sidebar next to the zoom buttons. Click and drag the joystick cursor in the middle of the screen in the desired direction to PTZ.

To use area zoom and click-to-center PTZ functionality, single click outside the joystick for click-to-center, or click and drag from outside the joystick circle to zoom into the selected area.



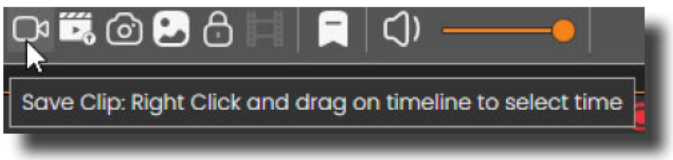
On-screen PTZ color themes can be changed by accessing the PTZ section of **Nexus Client Options**. Click the drop-down selection under On-screen PTZ to choose from the available options, then click **Apply**.



©2021 Airship Industries

EXPORTING A CLIP

The **Save Clip** button in the top toolbar gives users options for exporting clips of video. Clips can be downloaded to a drive on your PC in various ways or clips can be burned directly to a disc.

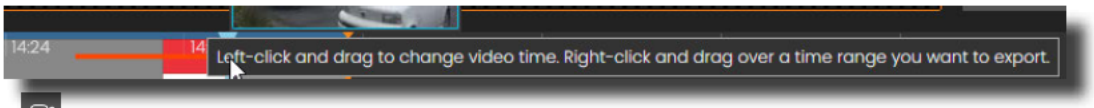


> 🕮 To burn a clip to a disc in **Nexus Client**, the user needs to have a disc loaded into your PC's disc drive or several discs loaded in your Rimage System's disc bins. The number of discs will depend on the amount of video being burned.

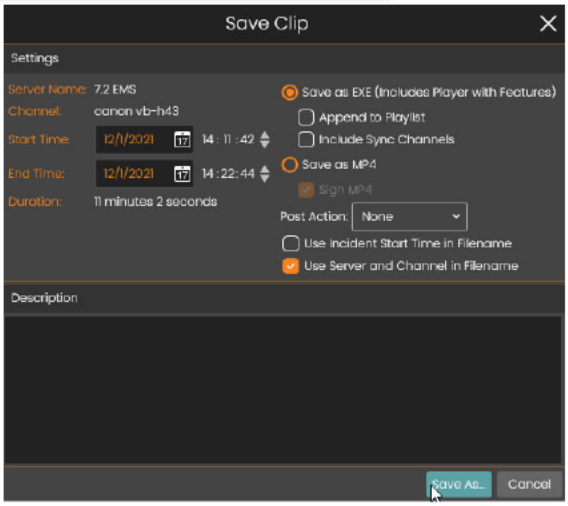
Saving Clips

Follow the steps below to save a clip to the default location:

1. In the **Video** tab, select the camera from which you'd like to export footage.
2. From the **Timeline tools** at the bottom, right-click on the timeline bar and drag for the time duration you wish to export. An orange line appears for the time period you select.



3. Click on **Save Clip** and you can see a list of options displayed.



You can choose the duration of the clip using the "**Start Time**" and "**End Time**" controls. For hard copies, you can also add the clip to a burn list or send it to Rimage Publisher from the options available.

Save as EXE: Leave this box selected to save the downloaded clip as a **.exe** file. This means the downloaded file will come packaged with a small piece of software which will give you some video-viewing tools.

Once exported and a file destination is chosen, you may select to assign a password, or skip.

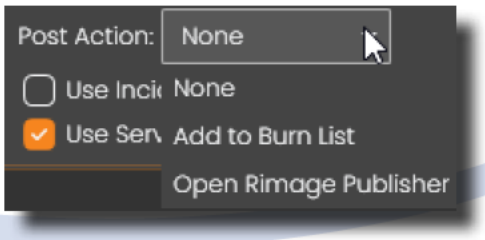
Check **Append Playlist** to add this exported clip to an existing clip in order to create a playlist.

To *export all* (max 4) currently synced video channels, check **Include Sync Channels.**

Save as MP4: Select this box to save the clip as a .MP4 file.

Sign MP4 By default, MP4 files contain a signature that authenticates when right clicking and checking the file properties, uncheck to remove this signature.

Post Action: If you select **Add to Burn List**, it will send it to **Nexus Client**s burn list, so you can click the Burn CD to download the video clip.
If you select **Open** Rimage Publisher, it will open after you export the clip. Using the Rimage Publisher, you can send your export clips to a new destination.



Description: Here you can add some details about the exported video for future reference.

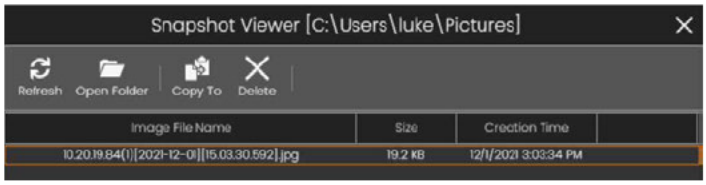
Save As: Select the **Save As** button at the bottom of the "Save Clip" window where you can save the clip to your desired location. Once you click **Save As**, the download will begin.

4. A new window will open allowing you to set a password with which to protect this clip.
5. Enter your desired password and re-enter to confirm the password, or you can skip the password protection step. This step is not required.
6. A new download window will open where the download for the selected video starts automatically and will result in an .exe file. You can pause or stop the download using the buttons for each download.

📖 **HELPFUL HINTS:** Users can set the default location for the downloaded clips under Options > Export > Save directory.

Snapshot Viewer

The **Snapshot Viewer** provides an interface for viewing and managing saved snapshots.



Refresh: Refresh the list of snapshots to pull snapshots taken by other clients on the same system.

Open Folder: Open the folder containing all snapshots saved to the current machine.

Copy To: Copy the selected snapshot to another folder on the current machine.

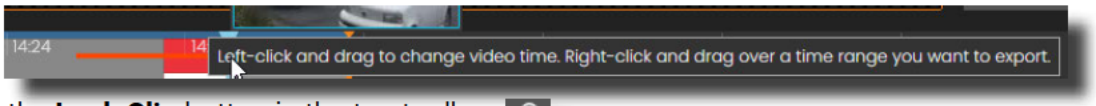
Delete: Delete the currently selected snapshot.

©2021 Airship Industries

Lock Clip

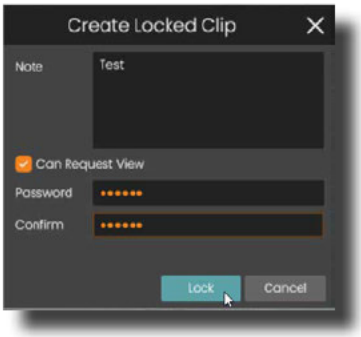
The **Lock Clip feature** allows users to create special permissions to access a particular clip. The following steps show the user how to **Lock a Clip.**

1. From the **Video** tab, right click and drag along the bottom timeline to select the desired footage for export.

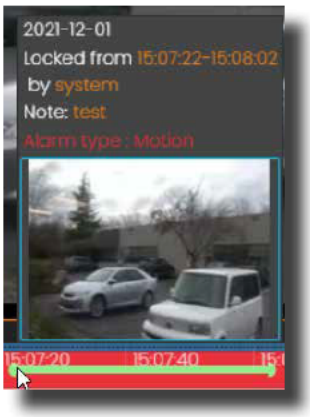


2. Click the **Lock Clip** button in the top toolbar. 

3. A **Create Locked Clip** option will pop up. Input any applicable information and click "Lock".



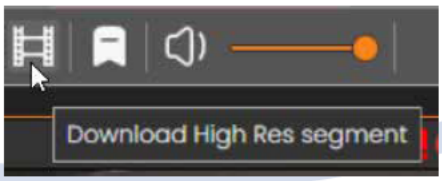
4. A **yellow indicator bar** will appear on the feed, and as you hover over the clip it will turn green..



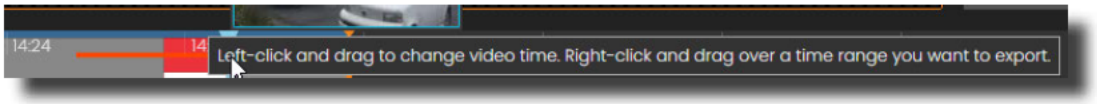
5. Only users with the same or higher permission levels can access locked clips. Users can unlock or modify the Locked Clip by right-clicking on the yellow indicator bar. Locking a clip will prevent the footage from being overwritten for the duration that it is locked.

High Resolution Download Feature

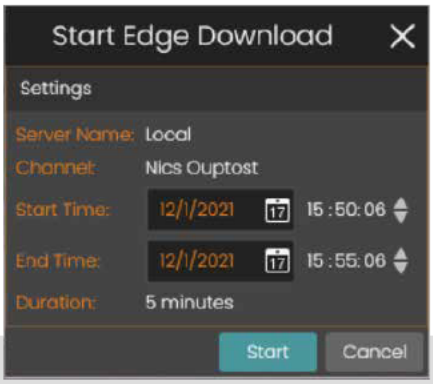
1. To download the high resolution footage from **Outpost** (stored on the edge recording device) to an Airship Server, click the High Res segment icon:



   a. Right-click on the recording timeline along the bottom of the client viewing window and drag the mouse over the duration of the clip that to be downloaded from the edge device (the process creates an orange bar visually indicating the clip duration as shown below). Then click **Start Edge Download**.



   b. Click the **Start Edge Download** button to select the start and end time using the pop-up window that follows, then click **Start**.

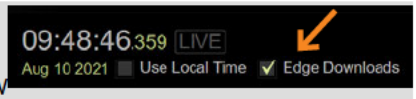


2. A warning popup will occur indicating that once a new download begins, and it will stop any existing downloads already in progress.
3. Click **OK** (or wait until existing downloads are completed), and a new pop-up window will appear indicating that the edge download is underway.

NOTE: In best practice, downloads should be performed during non-critical recording times, as the bandwidth used during download procedures may affect live streaming and record quality.

4. Once the edge download is finished, the high resolution clip can be viewed by scrolling over the section in the recording timeline indicated by the yellow line running through the middle of it.

NOTE: The high resolution clip downloaded from the edge and streamed (low resolution) footage may be downloaded separately by clicking the "Edge Download" button below the timeline. Streamed low resolution footage is left unaltered and is useful as the first copy for evidentiary purposes.



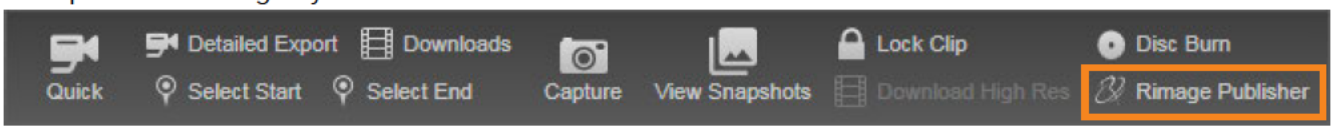
Once it is complete, you can either view the video on the disc or remove the disc by selecting "Eject when finished".

©2021 Airship Industries

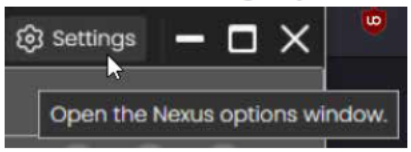
Rimage Publisher

Upon exporting video, if the user selects "Open Rimage Publisher" from the Post Action options, the following screen will appear after exporting.

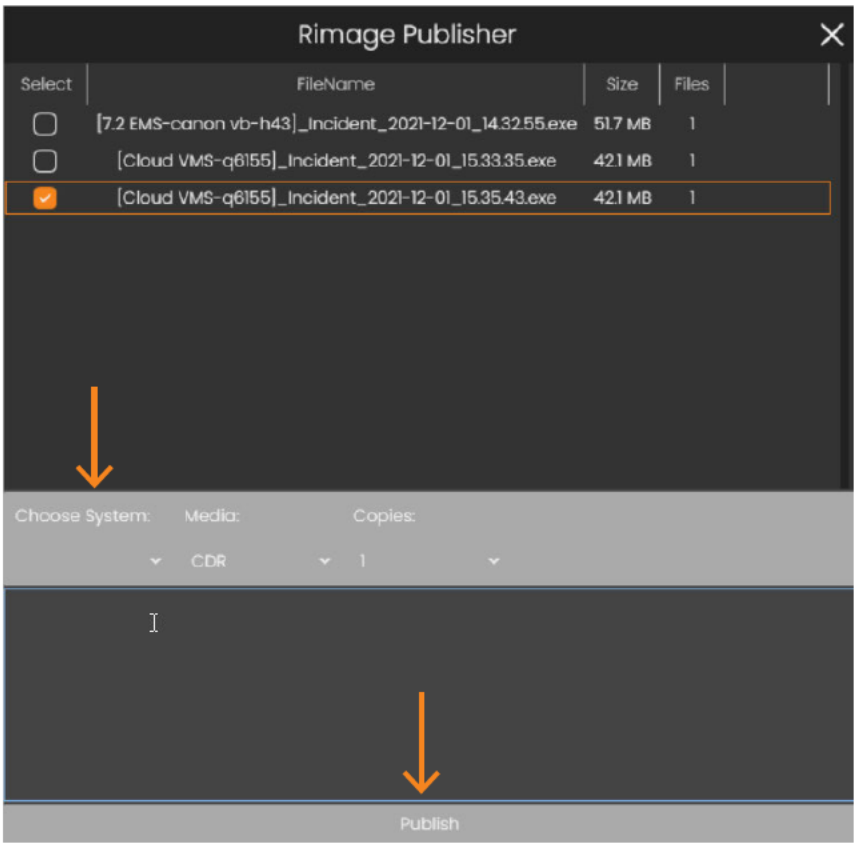
Users can send downloaded clips to their Rimage System to be burned to discs. Follow the steps below to send video clips to the Rimage System:



1. Go to **Settings** > Rimage Publisher to add a new Rimage System.



2. Click the **Rimage Publisher** button if a Rimage System already exists.
3. The **Rimage Publisher** window opens with a list of all downloaded clips.
4. Select the desired clip(s) and choose the previously added Rimage System.
5. Using the **Media** dropdown, select the type of disc you would like to burn to.
6. Select the number of copies you would like.
7. Click **Publish**.



CREATING CUSTOM VIEWS

Users can create custom views to produce a customized layout for their cameras. Views can be created in the **Video** tab or the **Views** tab. Views are synced across **Nexus Client** and Nexus Video Portal, which means any views created in **Nexus Client** can be used in Video Portal, and vice versa. These views are tied to the currently logged-in user.

Using the Video Tab

Views are screen configurations that can be loaded using a drop-down selection in the Video Toolbar.

Creating a View in the Video Tab:

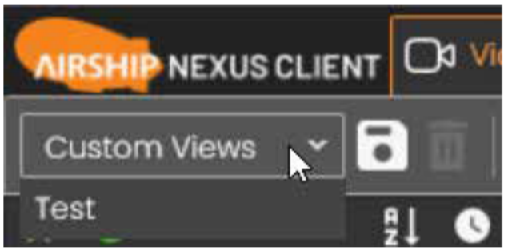
Follow the steps below to create a new view:

1. Open the **Video** tab and select the desired number of screens from the drop-down selection of **subscreens** in the video toolbar.
2. Add the desired cameras to each subscreen by just dragging the camera from the Assets list on the left onto each subscreen.
3. Click the **Save View** button in the toolbar as shown in the screenshot below. You can save the new view with a name for easy access.
4. The newly created views are available under the **Custom Views** drop-down in the video toolbar.

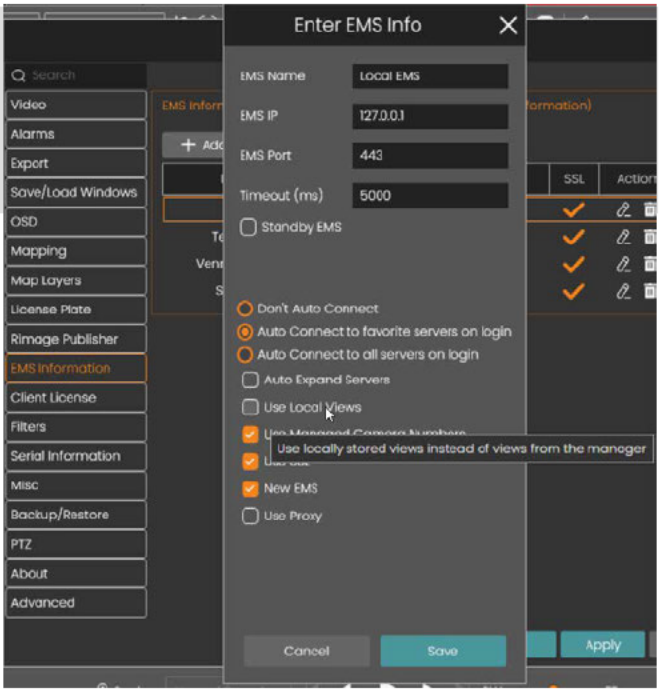
Toolbar Options

Save View: Clicking the **Save view** button will save the current layout of cameras displayed on the video screen as a **view**.

Custom Views: This dropdown will display all the views created by the logged-in user.



📖 **IMPORTANT:** If the Server is in Managed mode, make sure that "**Use Local Views**" is checked under **Nexus Client's** "**EMS Information**" options. Click edit on the desired Server, if "**Use Local Views**" is not checked, upon next login the view will be deleted.



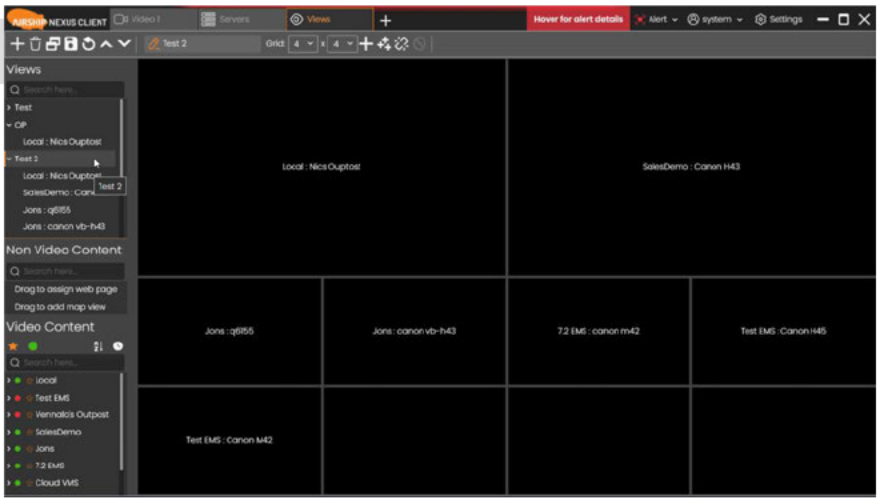
©2021 Airship Industries

Using the Views Tab

The **Views** tab allows the user to create and organize new views as well as add and remove cameras from existing views. You can see a blank screen in the design area when you open the **Views** tab for the first time as shown in the screenshot below.

📖 Collapse the arrow of Assets List to give more space for View Design area.

In the **Views** tab, the center area is called the 'View Design Area'. The Views panel on the left side shows all the existing views along with their associated cameras. Drag the cameras to the design area to view the video from them. You can also select the grid configuration for the design area using the Views Toolbar available at the top of the window.



Toolbar Options



Add: Click the **Add** button to create a new view. A new view gets added to the Views list on the left side. A yellow line precedes the newly created view to differentiate it from the available views.

Delete: Select a view from the list of views then click **Delete** to remove it.

Clone: Select a view and click the **Clone** button to create a duplicate view. Once you create a copy, they are simply two different views that can have different screens display various grid configurations.

Save: The **Save** button saves the changes made to the current view.

📖 **IMPORTANT:** If a view is currently open and has unsaved changes, you will be prompted to save it before creating a new view.

Revert: Revert will undo all the changes for the most recently changed view.

Move Up/ Down: Selected Assets will move up/down once in the list.



Grid: Grid allows you to select the number of rows and columns in the selected view's screen grid. You can change the view grid configuration at any time.

Add Subscreen: A newly created view has a blank screen. You have to add subscreens to your view. You can add multiple subscreens to a view based on your grid selection. If you try to add a subscreen when there is no more space, you will be prompted with an error message saying, "Out of Space". You can either remove the existing subscreen or increase the number of rows/columns in the grid to add a new subscreen. You can resize a subscreen by dragging on one of its corners.

🕮 **HELPFUL HINTS:** Remove a subscreen from the design area by clicking the close box at the corner of each subscreen.

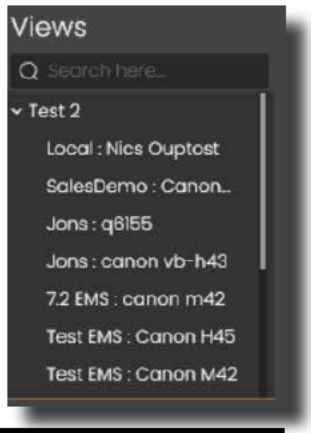
Fill Grid: The **Fill Grid** icon will fill the display area with subscreens based on the grid chosen.

Disconnect All: Clicking **Disconnect All** will remove all cameras from their subscreen views.

Clear Selected Subscreen Content: Select a subscreen in the design area to remove the camera attached to it.

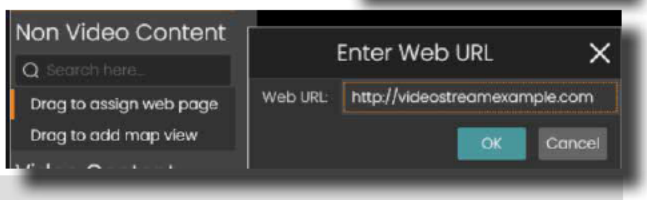
Views

The **Views** panel shows a list of all existing views. A user can call each view to see the cameras associated with that view.



Web Page

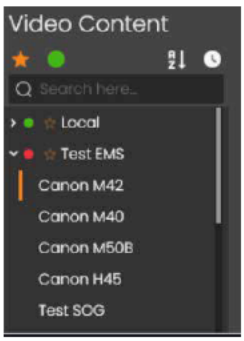
The Web page allows you to launch a web URL to the **View** screen instead of a camera stream. For example, instead of adding a camera to the subscreen, you can add a live video stream URL or website.



🕮 **IMPORTANT:** Click and drag to assign the web page, then enter the URL and click **OK**.

Video Content

Video content will give a list of all servers listed in **Nexus Client** and their associated cameras. All these cameras are available for loading to your subscreens. Select a camera and drag it on the desired subscreen to view its video. Video will not display in the **Views** tab but when you choose the view from the **Video** tab, the video content or the web content will be displayed.



©2021 Airship Industries

SAVING DEWARPED VIEWS

The **Saving Deparwed Views** feature allows users to save a preferred dewarped angle and have it reload instantly upon restarting or opening **Nexus Client**. The following steps show the user how to setup **Dewarped Views**. **Save a Dewarped Angle**:

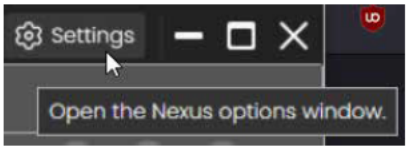
1. From the **Video tab**, click the **Dewarp option** on the bottom portion of the PTZ settings. Clicking this icon applies fisheye dewarp settings to the selected camera. Click the drop-down menu to reveal additional dewarp options.



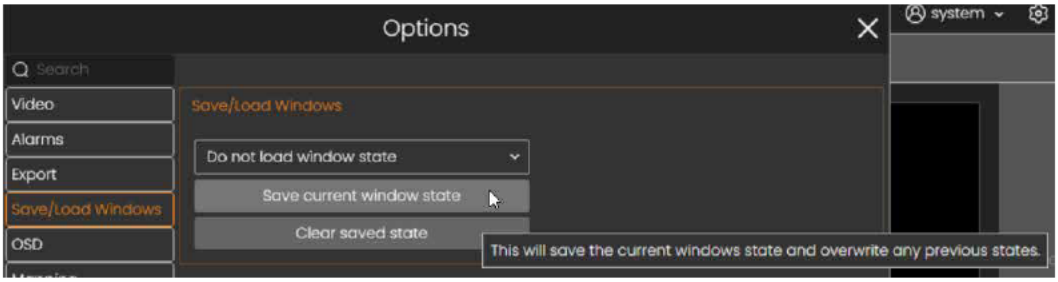
📖 **FEATURE**: The "**Quad View**" button will split the field of view on the selected screen into 4 dewarped views.

📖 **IMPORTANT:** After clicking **Dewarp**, the default option on the drop-down menu below Dewarp will be the **Ceiling** option. The Dewarp drop-down menu includes "Wall", "Table", "Panorama180", "Panorama360" and others.

2. Once the **Dewarp option** is chosen, click the **Settings Gear icon**.



3. Select **Save/Load Windows** from the left menu options. Click **Save Current Window State** to save the dewarped angle and then click **Apply**.

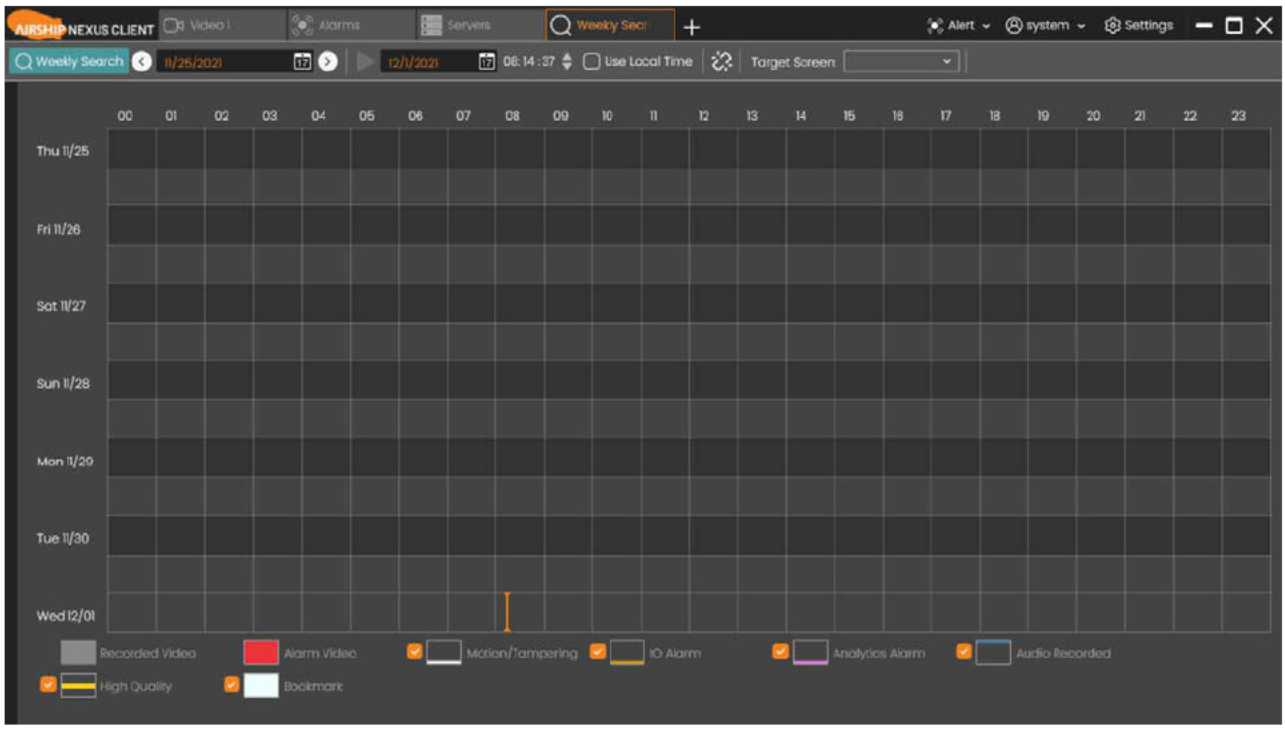


📖 **IMPORTANT:** if the user wants to load the Saved Dewarped upon restarting or opening **Nexus Client**, check Load Window State on Startup.

SEARCH FOR RECORDED VIDEO

Using the Weekly Search Tab

The **Search** tab allows the user to search for recorded video and alarm recording from multiple cameras, across multiple days, in one place. The grid view displays the timelines from selected cameras in a weekly view. You can move from week to week quickly using the search and calendar options in the Search toolbar covered below.

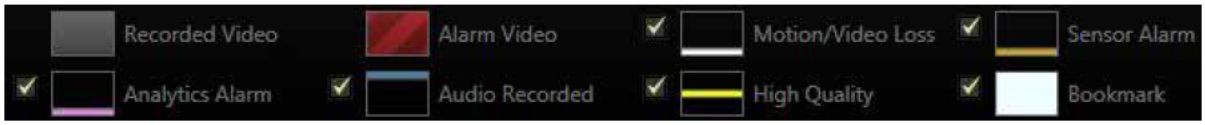


> 🕮 **HELPFUL HINTS:** Collapse the Assets list to give more space for the display area. Collapse the **Search Toolbar** using the arrow available at the right to give more room for the display area.

At the left side of the **Search** tab, each camera you select will be highlighted with a yellow line preceding it. Once the search is complete, a blue dot before all the selected cameras indicates that there is timeline information for those particular cameras from the previous search.

The different types of information you can see in the timeline are: Video, Alarm, Motion/Video Loss, Sensor Alarm, Analytics Alarm, Audio, High Quality, and Bookmark. Video and Alarm are displayed by default when you search for a particular camera. You can select from the other options whether you want to see that information or not.

Click the box beside each option to select or deselect them as shown in the screenshot below. After a search is complete, you can click to select or deselect individual cameras and the timeline grid will only show information associated with the selected cameras.



©2021 Airship Industries

Toolbar Options



Search: Click this button to search for recorded video after you select cameras. You can see the status bar for the search at the end of the toolbar as shown in the screenshot below. You can stop the search at any time using the **Cancel** button beside the status bar.

Calendar: Click the Calendar to select the start date of the week to search for video information. After you select the week, click the **Search** button. Once you select a date, you can also go to the previous week or the next week using the white **Prev** and **Next** buttons.

Play Selection helps users to quickly view the footage for the selected cameras using date and time options. Once you select the cameras from the list, choose the date and time and click the **Play** button to view the footage for all the cameras in the **Video** tab.

Play: Click this button after selecting the desired cameras, date, and time.

Date: Select a date from the calendar to view the footage from that date.

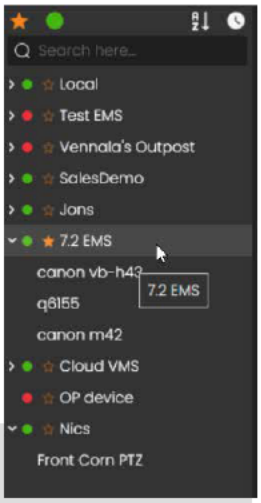
Time: Choose your desired time on the selected day using the up and down arrows.

Display Client Time: If you have servers located in different time zones, the timeline will show the time according to your client machine's local time, not the video server's local time."

Unselect All: Click this button to unselect all the selected cameras for search. A blue dot before all the selected cameras indicates that there is timeline information for those particular cameras from the previous search. You do not need to re-run the search in order to see the timeline of that camera incorporated into the grid.

Assets

The **Assets** panel is made up of two tabs: **Servers** and **Favorites**. The **Servers** tab shows a list of all servers in **Nexus Client** along with their associated cameras. All these cameras are available to search. Select the desired camera(s) and start the search. You can select/ deselect a camera to search by clicking on the camera name.



The **Favorites** tab shows all servers that have been chosen as "Favorites", making the most used servers easier to find. To add a server to the favorites list, either right-click on the desired server and choose **Add to Favorites** or navigate to the main **Servers** tab in **Nexus Client** (not the Assets panel **Servers** tab) and check the **Favorite** box on the line of the desired server. Just as with the **Servers** list, the **Favorites** list is also searchable using the search box at the top of the list.

📖 **HELPFUL HINTS:** The assets list can be filtered in **EMS** by location and/or permissions. This will decrease the number of servers and cameras being connected to upon launch of **Nexus Client**, thereby significantly decreasing connection time for a faster launch.

Calendar

The **Calendar** at the bottom of the **Search** tab will highlight the day with a red circle where there is recorded footage. You can choose the first day of the weekly timeline either from the calendar in the search toolbar or the calendar at the bottom of the window. Double-click on a date to start the search for that date. Current date is highlighted in green.

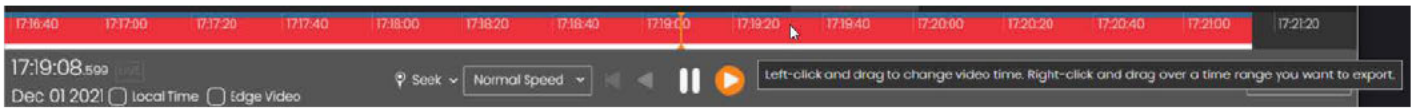


📖 When you have multiple cameras selected to search for recording, the calendar will highlight the date(s) in red where there is footage from those cameras, even if there is footage from only one of the cameras.

Using the Video tab

The user can easily view footage from a selected camera using the playback controls provided at the bottom of the **Video** tab.

Timeline Tools



Timeline bar — At the bottom of the **Video** tab, the timeline gives the user control over the playback video. For the selected camera in the camera list of the **Search** tab, a user can see the playback information in the **Video** tab's timeline bar. You can move the timeline forward or backward to seek to a new time/date. It allows the user to play the video at the desired speed using different options for playback.

In the timeline bar, white indicates motion, red for alarm, blue for audio, and gray is the video. Black shows when there is no recording. A yellow marker with this symbol indicates the current time marker.

Timeline View: — Select the time duration to display in the timeline bar. Default value is set using "Default Timeline View" covered on page 48..

📖 **IMPORTANT:** For daylight savings time, select the camera that has recording during the DST hour and click the DST Hour checkbox on the timeline. Users can toggle between normal playback and the lost hour using this checkbox.

Local time: — Check to display local time when the client is displaying video from a different time zone.

Time: — For a selected video, time is displayed either for live view or playback.

Seek: — Seek allows you to view the playback for a selected date and time. Click this option to open the calendar to choose the date and time. Click the **seek** button beside the time to complete the attempt to search for the desired date and time.

©2021 Airship Industries

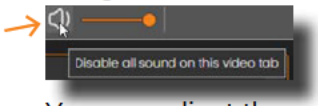
Speed Select: There are two ways to select the speed to view footage. One is the drop-down to choose the playback speed, and the second is the rewind/forward bar. Using the rewind/forward bar, you can scrub through the video while the selector is held in a particular location on the bar. Playback speed will correspond to the speed indicated, and the video will pause when you release the slider.

📖 **NEW FEATURE:** Double clicking a date on the **Seek Calendar** will automatically seek to date clicked.

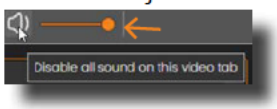
Channel Audio: Select a subscreen and click the mute button to mute the sound for that particular channel. Click the button shown here:



Audio: You can mute/un-mute the audio for all the channels in the current video tab using this button.



Volume bar: You can adjust the master volume with this slider.



📖 **FEATURE:** An indicator was added next to the time stamp to show whether the video is Live. The LIVE button will be green when live and grey when not. Moreover, the Live button can be clicked to jump from recorded video to Live video when viewing Live video.



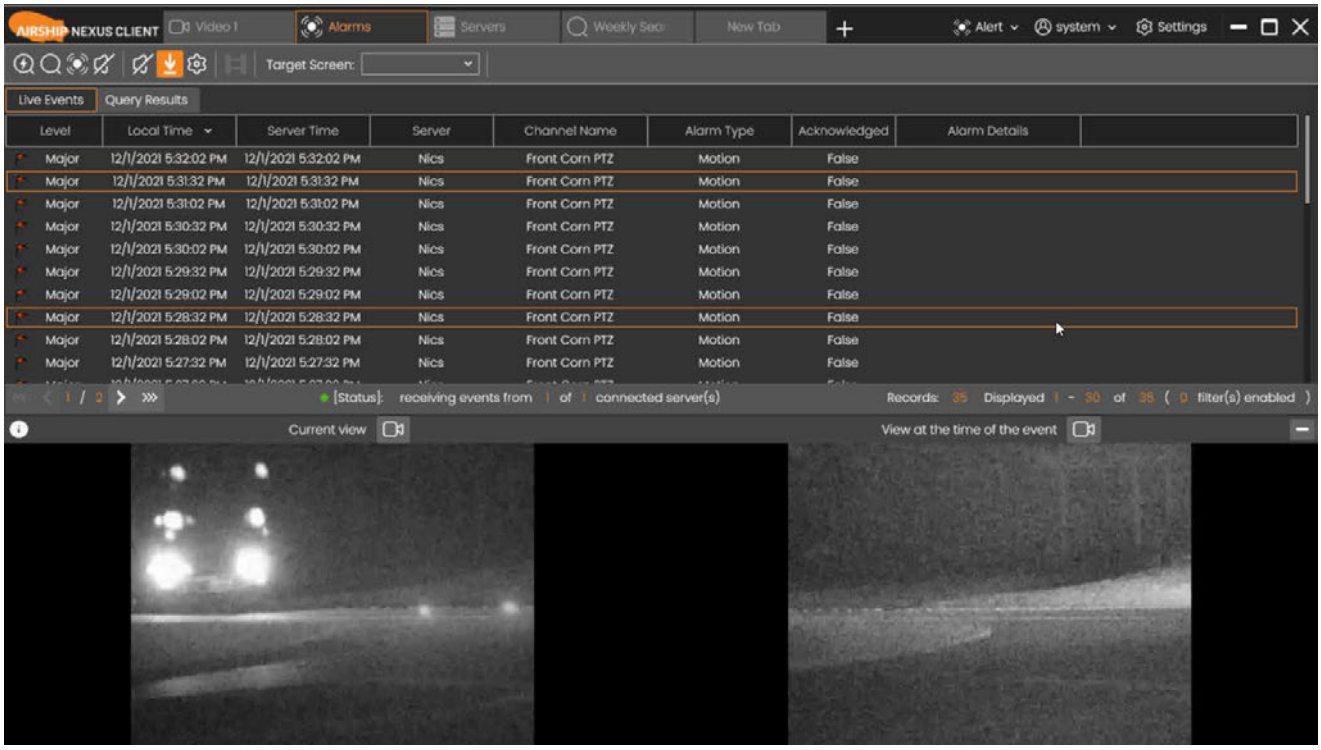
ALARM CONSOLE

The **Alarm Console** tab displays alarm messages from Airship Server. The alarms come from the Metadata Server component of the Airship VMS, which means that an Airship Server needs to have the Metadata Server running to send alarms to **Nexus Client**.

Alerts from Airship Server can be collected by a Metadata Server and managed with the **Alarm Console** tab. A System Administrator can generate reports based on Alarm type, Server, Severity, etc.

> 🕮 **IMPORTANT:** You can open only one **Alarm** tab at any given time. A red light flashing on the alarm button signifies an incoming alarm, and it keeps flashing until there are no alarms being received by the client.

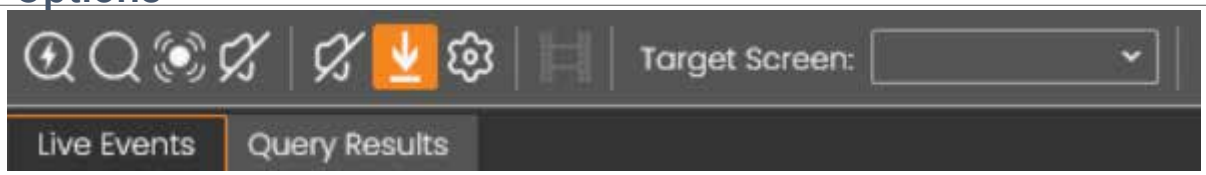
On the **Alarms** tab, current alarms are displayed with the most recent at the bottom of the page. In the list of alarms, users can see information such as Alarm Level, Client Time, Server Time, Server Details, and Alarm Type for each alarm received.



Double-click an alarm in the list to see the live video from that alarm as well as the video at the time **Nexus Client** received the alarm. See the above screenshot for an example. Press the letter 'L' using your keyboard to open the live view in the **Video** tab. Press the letter 'P' to show the playback of the video in the **Video** tab.

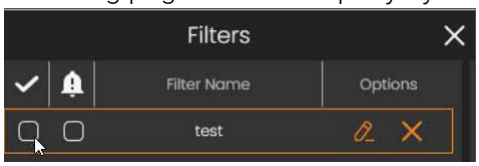
©2021 Airship Industries

Toolbar Options



Quick Search To quickly populate the existing alarms, click this feature.

Search with Filters: Search with a new or existing filter for previous alarms. You will see a pop-up window once you click the **Search with Filters** button as shown on the following page. Clear the query by deselecting the check box on the left.



Acknowledge: The user can remove the alarms from the list with an acknowledge command.

Stop Alarm Click to stop an active audible alarm.

Recent: The **Recent** button helps you see the current alarms with the latest at the bottom.

Select Filter: Create, edit, or add new filters with the filter tool. See **"Alarm Filter Options" covered on page 34**.

Edge Download: Click to download footage from the Edge device based on the alarm event selected.



Target Screen: Select the screen from which to filter results.

Live: When the **Live** toggle is ON (enabled) you can see the fresh list of alarms. When this feature is OFF, new alarms coming in will no longer be shown.

Query Results: View alarm events based on the last Query results. Click the column headings to sort.

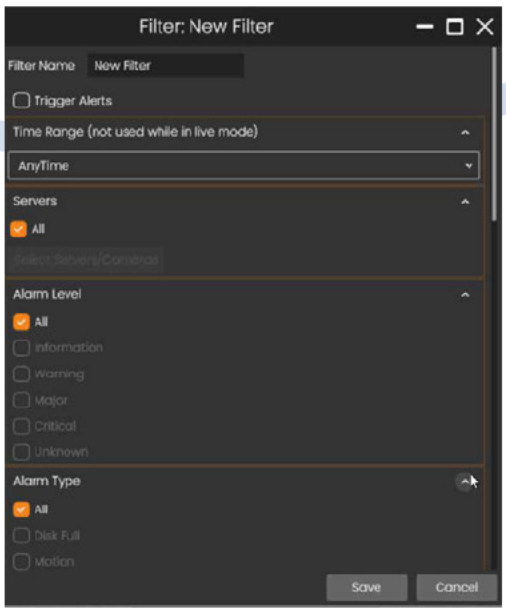
Alarm Filter Options

Click the Filter button to reveal Filter options, then select which values to filter by.

Trigger Alerts: Uncheck this box to search for alarms which are not acknowledged by the Server, but only by Nexus Client.

Time Range: You can choose the time for which you want to see alarms. You can view for the last hour, last day, last month or select from the calendar using "Custom range...".

Use Local Time: You can search for alarms using client time rather than the time zone local to the server.



Select Servers/Cameras: You can search based on the servers or cameras connected to the client. Choose a server from the list of available servers or cameras to view all the alarms received from that server or camera.

Alarm Level: Alarms have varying levels of severity. Under "Alarm Level" select the severity of the alarm: Information, Warning, Major, and Critical.

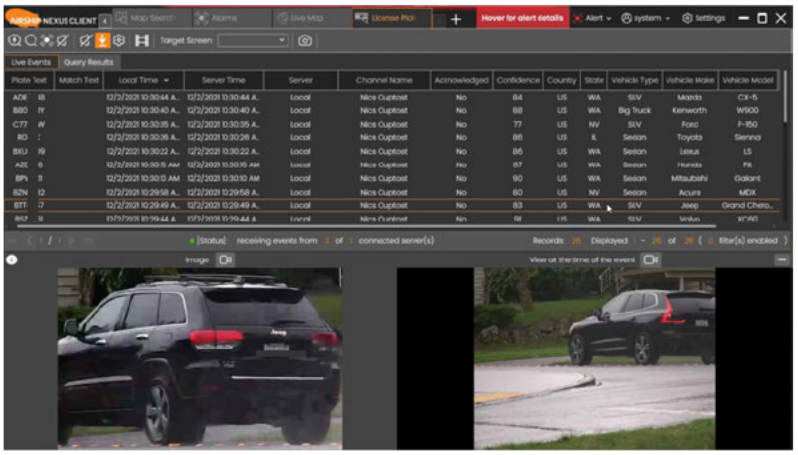
Alarm Type: You can choose from the 13 Alarm Types available. They are: Disk Full, Motion, MotionEnd, IO, IOEnd, VideoTampering, VideoTamperingEnd, VideoLost, VideoLostEnd, Custom, CustomEnd, VideoFileOpen, and VideoFileClose. If you receive any alarm other than the above mentioned, you can view those alarms by selecting the "Unknown" option from the list of Alarm Types.

©2021 Airship Industries

LICENSE PLATE SEARCH

Automatic License Plate Recognition (ALPR) allows the user to collect license plate data from a camera connected to the Airship Server. **ALPR** uses **Optical Character Recognition (OCR)** on the incoming image. It then sends its best matches off to the **Metadata Server** for storage.

You can then use advanced search options to search for an individual plate, text, time, camera, etc.



Full setup and advanced instructions for **Advanced License Plate Recognition** can be found in the *ALPR Setup Configuration Tool Guide* and the *ALPR User Manual*.

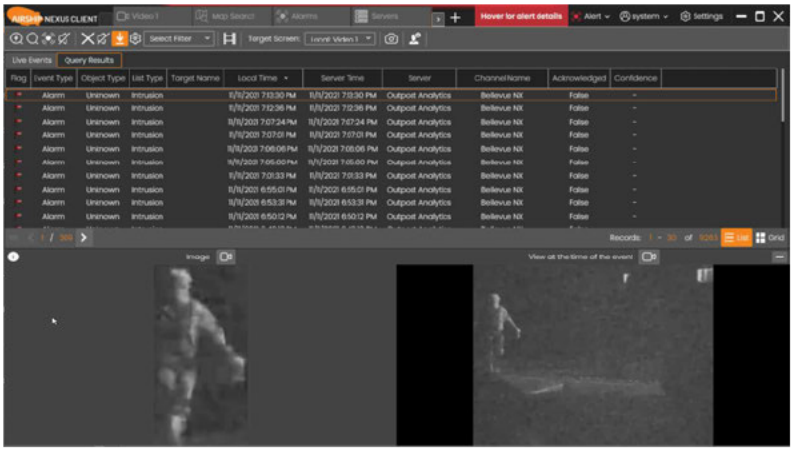
> 🕮 **HELPFUL HINTS:** Double-click on a license plate to open the playback video for that recording in the Video tab.

FACIAL RECOGNITION

Airship provides native integration with select facial recognition engines, allowing **Nexus Client** to display facial detection and recognition metadata along with resulting alarms in a single pane of glass.

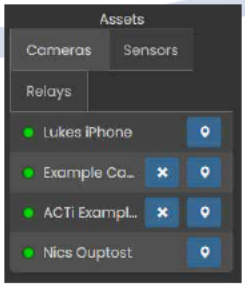
Live and recorded metadata will be displayed on this tab. Upon opening a new **Facial Recognition** tab, select **"Quick Search"** for a list of all your results sent to **Airship**, or you can click "**Live**" and **Nexus** will monitor and notify you of any new alarms.

For complete setup instructions, please see the *Facial Recognition Setup Guide*.



MAPS

A great way to visualize camera placement, orientation and control is with Airship Map features; E-Maps, Live Map, and Map Search. These three tabs are covered in the sections that follow.



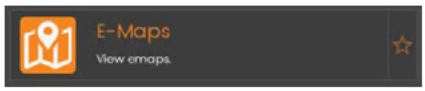
E-Maps is a tab built for camera orientation and placement laid over blueprints, maps or other layouts, great for large or complex building layouts when you need to quickly understand which camera is best to view an event. Use the E-Maps options available within the **EMS** UI to insert layouts, place and orient cameras, and save layouts.

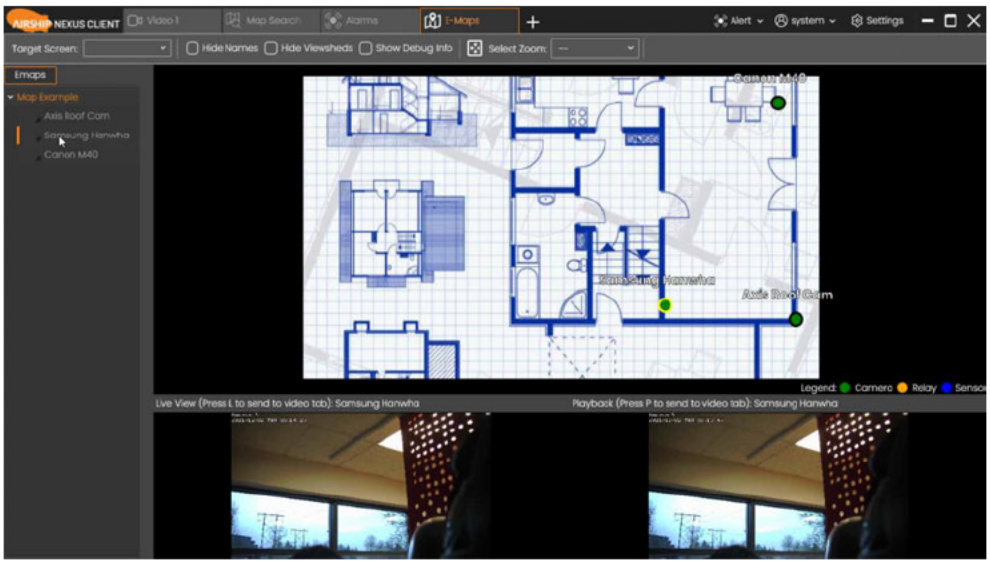
For live viewing, panning, tilting, zooming, as well as GPS tracking, the Live Map tab works as a way to view and manage cameras from a map view. Sensors such as worn body-cameras or PTT radios may be tracked and displayed to show location data. See the section "Live Map" covered on page 37.

For viewing events and playback history of GPS tracked it**EMS**, use the Map Search tab.

E-Maps

From **EMS**, maps can be uploaded and cameras may be assigned to them. Nexus Client displays these maps and their assigned cameras in the E-Maps tab. Double-clicking the marker will display the video from the selected camera on a Video tab.





A legend appears below the map, displaying the device's status. Above the map, viewing options are available in the ribbon.



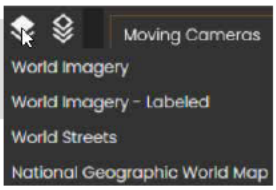
Target Screen:	Select the screen from which to load associated maps.
Hide Names:	Check to hide camera/device names.
Hide Viewsheds:	Check to hide viewshed area (set in EMS) from displaying on the map view.
Show Debug Info:	Check to display camera/device debug info, which appears on the right of the ribbon.
Select Zoom:	Select to scale map.

📖 Note that the E-maps tab is only displayed for EMS users in Managed Mode.

©2021 Airship Industries

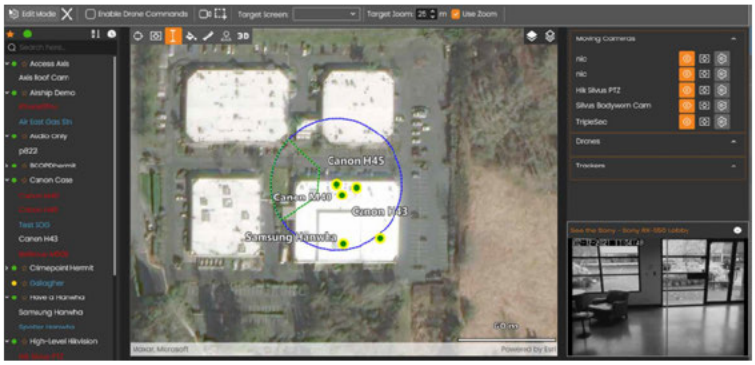
Live Map

Using the **Live Maps** tab, you can view the current location or direction each camera is facing. Drag and drop cameras and/or sensors to be placed on a map or have it be automatically plotted based on it being GPS capable (and integrated).



📖 **FEATURE:** Select from map overlays by clicking the maps drop-down at the top right of the map's viewing window (shown on right). Feature layers may be added in Settings.

1. Click the Drag Select icon to drag and select multiple cameras at once.
2. Click the Open Video icon to open all selected cameras to a viewing screen.
3. PTZ cameras can reposition based on clicks from this screen. Click the camera's viewshed to redirect the selected camera.



📖 When more than one PTZ camera shares a "viewshed" (the total viewable field-of-view), you may double click on the shared portions of the viewshed to quickly point all cameras in the same direction.

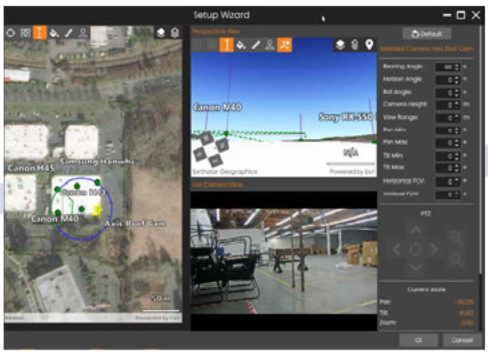
Toggle on/off viewing devices and features with the orange eye button.



For further mapping setup instructions see the ***Silvus Radios & PTT Quick Reference Guide***.

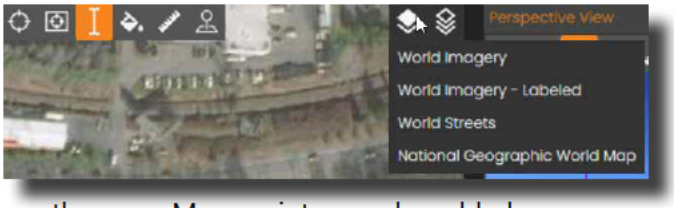
GPS integrated devices such as bodyworn cameras, mobile cameras, radios, or iPhones running Mobile Encoder can all be tracked using the Live Map tab. Such GPS enabled devices will appear on the map and leave a trail of "breadcrumbs" which may be viewed in the Map Search tab.

Use Setup Wizard to Orient Cameras/Devices



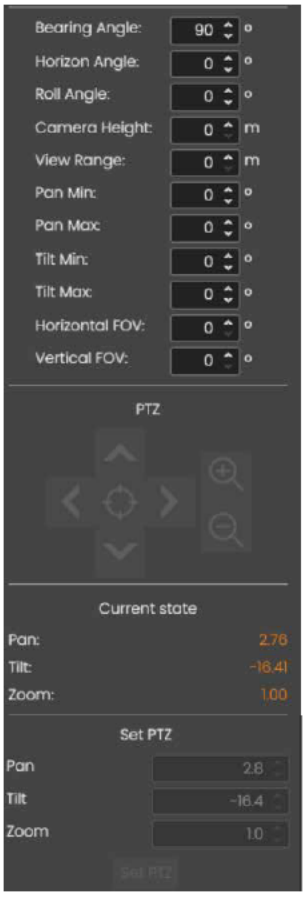
Click **Edit Mode** in the top left of the **Live Map** tab to configure orientation and calibration settings for the selected device or camera. Clicking the **Setup Wizard** icon will display 2D and 3D maps to help orient the camera's view with the map view.

From this Setup Wizard, the Bearing Angle, Horizon Angle, FOV and other orientation settings may be manually entered in to match the physical dimensions of the camera's view. Icons in the top of the 2D map view will perfom the following:



- Click to center the 2D view around all objects.
- Click to center around the selected object.
- Click to toggle on/off labels.
- Click to toggle on/off shape fills.
- Click to measure distance and angle between two points on the map. More points may be added or removed by right clicking while the measurement tool is active.
- Initial click displays the current coordinates based upon where the map is centered. Click to manually enter coordinates for the map to center over. Use the drop down to choose between alternative GPS coordinates other than the default lat/long/deg/min/sec.
- Click to load 2D feature maps, more maps may be added. Feature maps for places and things of interest may be uploaded. More information on this is covered in Mapping on page 52.
- Click to load 3D feature maps. See "Map Layers" covered on page 53.

To save the changes, exit out of the window, and a prompt will appear asking to Save or discard changes. Click Yes to save.



Bearing Angle: Adjusts the compass direction from the point of origin and measures angle counterclockwise.

> 🕮 **NOTE:** 0° equates to "East" (as shown by the compass icon on the bottom of the PTZ options), and Pan degrees are set in comparison to the Bearing Angle; i.e. If the camera actually faces West, set the Bearing Angle to 180° to properly calculate Panning degrees.

Horizon Angle: Relative viewing angle to horizon; default 0°.

Roll Angle: Relative angle of rolled view; default 0°.

Camera Height: Adjusts accuracy of FOV figure icon to match camera height in the real world.

View Range: Sets the maximum range can reasonably see (in meters).

Pan Min/Max Sets Pan (left/right) limit values

Tilt Min/Max Sets Tilt (up/down) limit values

Hoizontal/Vertical FOV Sets the maximum angles for field-of-view.

Current Pan/Tilt/ Zoom Displays Pan, Tilt, or Zoom values, click the up/down arrows to adjust manually.

Set PTZ Click to send manual adjustments to the camera selected.

©2021 Airship Industries

Edit Mode Disabled

Edit Mode is off/disabled by default, while off, it allows the user to manage display options.

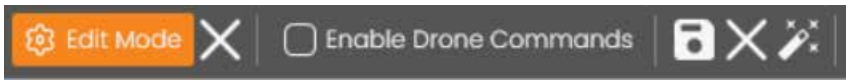


Edit Mode:	Enable to make changes to the placement, selection, and/or PTZ settings of the cameras on the map.
Enable Drone Commands:	Commands sent via Nexus Client to connected drones are active with this check box enabled.
Goto Position:	Enter lat/long coordinates if known to navigate to the desired area of the map.
Open Video:	Open the video from the selected camera.
Drag Select:	To select multiple cameras at once, select this option, or right click on the map to drag a box around the desired cameras.
Target screen dropdown:	Select the screen to which you would like the selected camera's video to be displayed in.
Use Zoom:	When enabled, when a user clicks in a camera's "Viewshed", the camera will zoom as well as pan and tilt. When disabled, the camera will only pan and/or tilt.

📖 **Note:** Additional metadata information associated with those devices can be provided such as lattitude and longitude. Bodyworn or mobile cameras, as well as PTT radio devices can then be tracked and displayed across the maps in real time.

Edit Mode Enabled

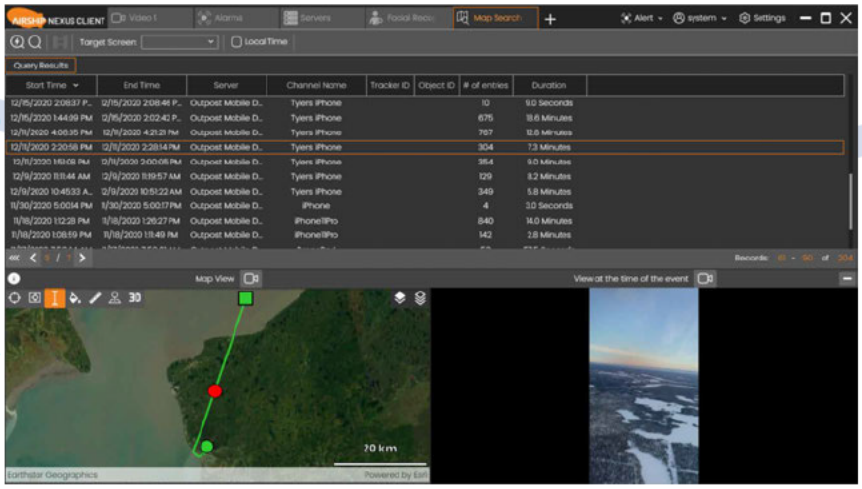
When Edit Mode is enabled, it allows the user to make changes to the placement, selection, and/or PTZ settings of the cameras on the map. With edit mode disabled, the options cover PTZ



Edit Mode:	This is a toggle for enabling and disabling Edit Mode.
Center All:	Center the map on all cameras on the map.
Center Selected:	Center the map on all selected cameras.
Deselect All:	Deselect all selected cameras.
Save:	Save the current configuration.
Remove:	Remove the camera from the map.
Default:	Return the selected camera's settings back to the default.

Map Search

To search the history on mobile camera or radio markers, select the **Map Search** tab. Click "Quick Search" to populate existing location events. Click an event or breadcrumb (location icon on map) to display the associated footage and stored metadata. Click the columns to sift/sort through results.



This process is covered in the ***Airship Mobile Encoder QRG*** or the ***Silvus Radios & PTT QRG.***

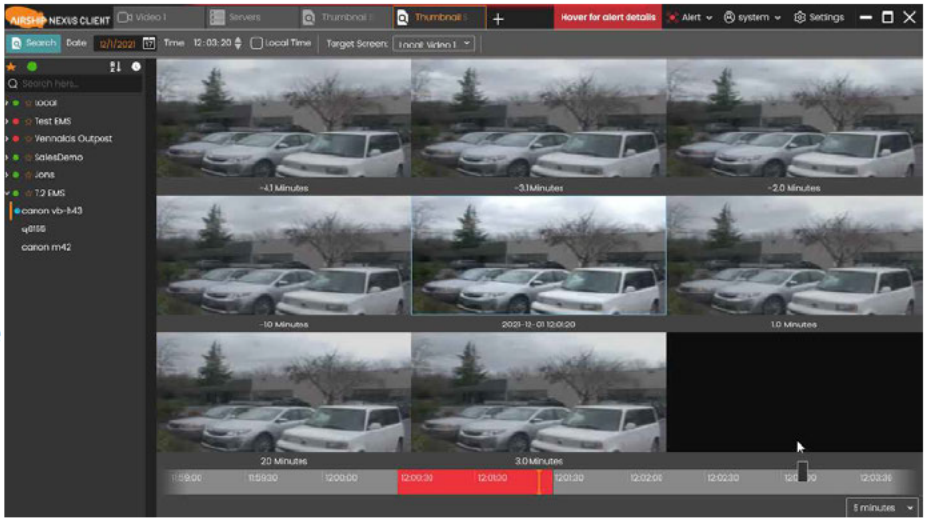
EMS

The **EMS** tab simply provides a browser window embedded into **Nexus Client**, and opened to the currently-connected **EMS**. This will be the **EMS** the currently logged-in user selected upon login.

> 🕮 The **EMS** tab will not be available if logged in using ***unmanaged*** mode.

THUMBNAIL SEARCH

When you need to quickly scrub through video, the thumbnail search tab helps you see multiple thumbnails at once. Click the Thumbnail Search tab from the New Tab page, or select any camera, and click the thumbnail search icon to open a new window that sorts through video by thumbnail.



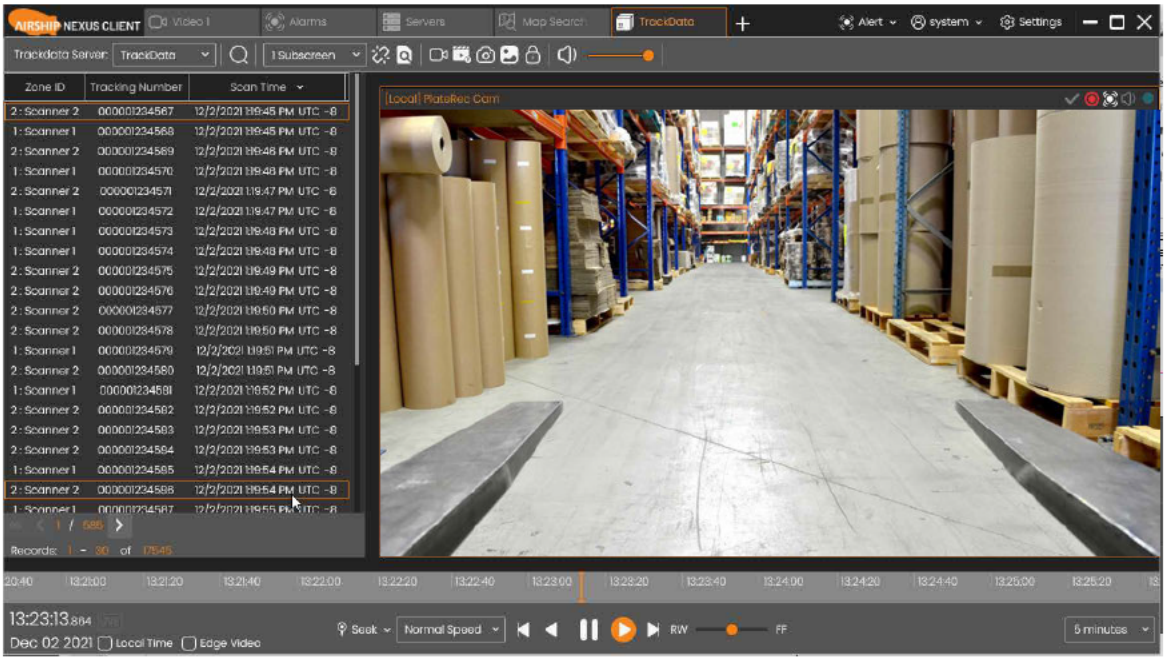
The middle screen shows you the current time where the cursor is placed. The footage displays oldest to newest thumbnails from top to bottom, left to right. Start a search by selecting a time and Target Screen, then select "Search".

©2021 Airship Industries

TRACKDATA

Nexus Client has a tab labeled **TrackData Client**. The **TrackData Client** provides functionality for tracking packages as they advance down the line of a shipping facility.

If a user needs to find a particular package, they can simply pull up the TrackData tab in **Nexus Client**, select a Server, type in the package's tracking number, and a list of the package's scans will be shown along with recorded footage of that package during each scan.



✓ **IMPORTANT:** For complete setup and configuration instructions, see the *Airship Trackdata Quick Setup Guide*.

Toolbar Options



Trackdata Server:	Use this dropdown to select the desired Trackdata server to connect to.
Find Package:	This button opens a dialog where the user can search the database for a specific package's records using its tracking number. This dialog also provides an option to filter by a certain amount of time.
Subscreen Views:	Select the number of subscreens to display in the viewing window.
Add/Edit/Delete Server:	An Airship Metadata Server needs to be running to provide results to the client. The **Add Server** button allows the user to enter the server(s) to connect this client to. You may also edit or delete a previously saved Trackdata Server.
Disconnect All:	Click the **Disconnect All** button to close all camera feeds on the current view.
Thumbnail Search:	This shortcut directs to the Thumbnail Search tab, displaying the currently selected camera's playback video across thumbnails.
Export	See "Exporting a Clip" covered on page 19.
Open Clip Exports Window:	Click to view the list of clip exports produced from Nexus Client.
Snapshot:	Saves an image of the selected video at the current time.
View Snapshots:	Views the snapshots taken from Nexus Client.
Lock Clip:	Click to create special permissions to access a particular clip. This feature is covered "Lock Clip" covered on page 21.

WALL DESIGNER

Wall Designer is used to create views and salvo designs which you can save for later use. **Salvos/Views** can be set to display any number of video streams to any combination of monitors with a single selection.

Wall Driver

The **Airship Video Management System (VMS)** package allows the user to see live video on remote work stations using **Wall Driver**. Users can connect a Wall Driver to one or more monitors. The **Wall Driver** program can display video streams from multiple video inputs (NVR/DVR) to the monitors.

The features of a **Wall Driver** are:

- Digital monitor display
- Analog and IP video display
- Up to 16 subscreens per screen

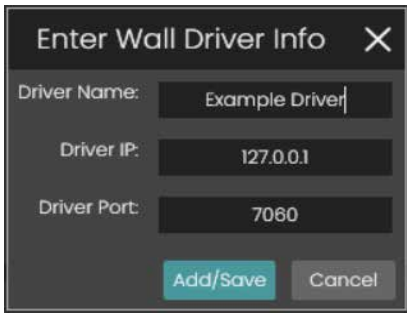
Add a Driver

You can add a **Wall Driver** in the **Monitors** column. Right-clicking in the monitor column will open a set of options where you will select "Add driver". This pops up a new window where you provide properties of the **Wall Driver** you want to add.

Driver Name: You can provide a unique name for the newly added Wall Driver.

Driver IP: Provide the IP address of the machine on which you have installed the Wall Driver.

Driver Port: Port number assigned to the Wall Driver.



©2021 Airship Industries

Toolbar Options



Controller Mode: Check this box to toggle between Wall Designer and Wall Controller mode.
Designer mode, you can create a new salvo and view as well as customize your screens and monitors.
Check **Controller Mode** to preview views and salvos created from Designer mode and take a tour on the salvos added.

Create Salvo: A **Salvo** is a layout of cameras on a number of specified monitors that users can quickly launch to see the preview of the camera layout. Click this button to create a new salvo. You can see the created salvo in the **Salvos** panel in the bottom-right corner of the Wall Designer window.

📖 **IMPORTANT**: If a salvo/view is currently open and has unsaved changes, you will be prompted to save it before creating a new salvo/view.

Create View: A **View** is a layout of cameras in a customized screen format that users can quickly launch to any single monitor. Click this button to create a new view. The screen layout (subscreens) must be selected to create a new view. You can see the created view in the **Views** panel in the bottom-right corner of the window.

Save: The **Save** button saves the currently open salvo/view.

📖 **IMPORTANT:** There can only be one unsaved salvo/view at any one time.

Save As: Select the Salvo/View from the **Salvos/Views** panel and click the “Save As” button to save it with a new name.

Test: The **Test** button allows you to check the newly created Salvo/View by launching it to your monitors. When testing a salvo, select the salvo from the **Salvos** panel in the bottom-right and click **Test**. When testing a **View**, select the view from the **Views** panel in the bottom right, select the screen you would like to test it on, and then click the **Test** button.

Refresh Status: When you create a new salvo/view, and you load cameras onto your screen, you can click **Refresh Status** to have your loaded cameras update the image within the **Wall Designer.**

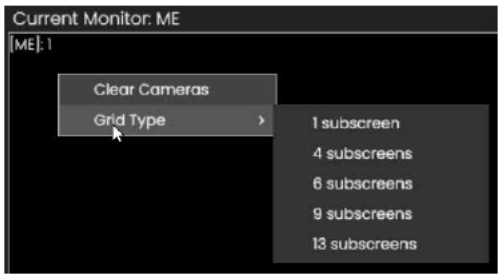
Current Monitor

The **Current Monitor** area displays the screen layout for the salvos/views of the monitor selected. Drag a monitor to the screen from the right-side **Monitors** panel. Add a camera from the **Video Content** panel to the screen. You can have up to 16 subscreens per screen, and they can be selected either at the time of creating a view or when you right-click on the screen. You can see the camera name displayed in the top right-hand corner of each subscreen.



Right-click Options

Right-click in the **Current Monitor** area to display different options for changing view settings. If you have more than one subscreen, you can select your desired subscreen to make changes. The selected subscreen is outlined with white.

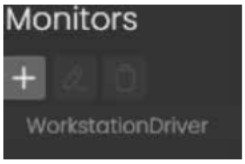


Clear Cameras: Removes all the cameras assigned to all subscreens.

Grid Type: You can select your desired number of subscreens from the given list.

Monitors

The **Monitors** column will display all the **Wall Drivers** added along with the monitors assigned to them. Select monitors from here and place them in the **Current Monitor** area to add cameras to them.



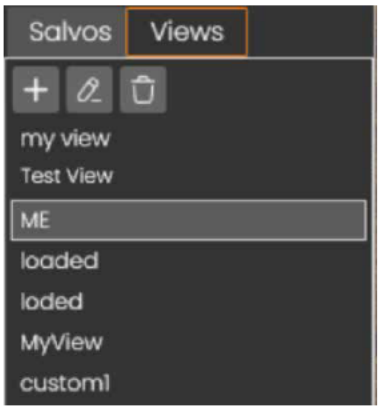
Right-click Options

Add Driver: Refer to the Add a Driver section for more information.

Refresh Driver: Refreshes the number of screens within the Wall Driver.

©2021 Airship Industries

Salvos/Views



Salvos: Lists all salvos created in the **Wall Designer** tab.
Select to view.

Views: Lists all views created in the **Wall Designer** tab.
Select to view.

Add: You can add a new view when you are editing a salvo.

Edit: The **Rename** option allows you to change the name of the salvo/view once you have created it.

Remove: You can delete a salvo/view from the list using the **Remove** button.

Right-click Options

Rename: The **Rename** option allows you to change the name of the salvo/view once you have created it.

Remove: You can delete a salvo/view from the list using the **Remove** button.

Reorder: **Reorder** allows you to change the order of the salvos/views displayed. A new window pops up, which is where you drag them to change their order.

Current Video Wall

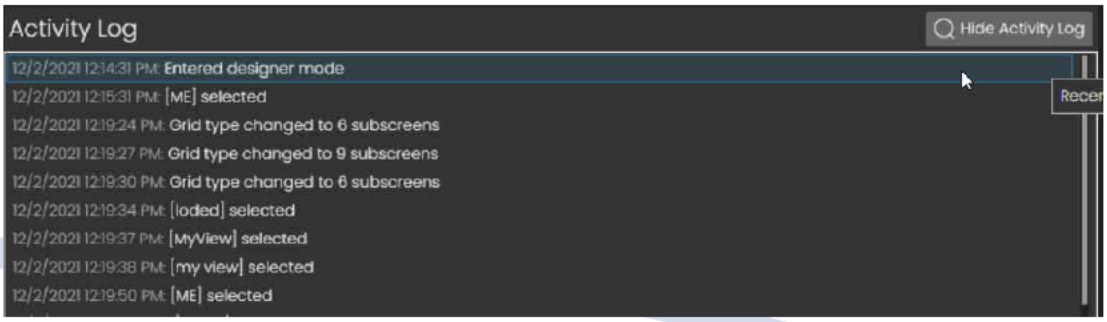
Current Video Wall This displays the monitors selected from the **Monitors** panel and displays them in the previously designed grid view. Drag the desired monitor and place it on a screen.

Add Screen: Click the **Add Screen** button to add the desired number of screens. You can see a blank screen and can add monitors to display them.

Grid Selection: Select desired grid size to view the monitors in the screens.

Activity Log

The **Activity Log** will display the log report for Wall Designer. You can hide the activity log at any time using the **Hide Activity Log** button.



WALL CONTROLLER

> 🕮 **IMPORTANT:** Refer to the 'Installation Manual of **Nexus Client**' for more information on Wall Driver installation.

Wall Controller sends camera configuration information to **Wall Driver**, which displays cameras and/or web pages on monitors. To begin, add cameras to your **Views**, assign **Monitors** to those **Views**, then assign **Views** to a **Salvos**. Users can launch **Salvos** and **Views** to display multiple cameras on individual or multiple monitors.

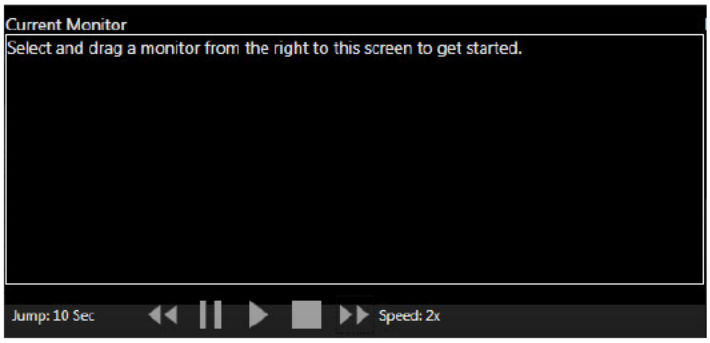
> 🕮 **HELPFUL HINTS**: The yellow bar in the center of the window can be dragged up and down to allow **Current Monitor** and **Current Video Wall** to have more space.

Toolbar Options

Refresh Status:	**Refresh Status** allows you to update the current screen, including the status of the video and a still image of the video on the screen.
Add:	Add a Wall Driver.
Edit:	Edit the Selected Wall Driver.
Remove:	You can remove a monitor, salvo or view from the list using the **Remove** button.

Current Monitor

The **Current Monitor** area is where you can add cameras after you select the monitor from the **Monitors** panel at the right. Below the current monitor box, you have options to rewind, pause, play, stop, and fast-forward the playback video.



Right-click Options

Right-click on the **Current Monitor** area will display different options that you can use to change the view settings. If you have more than one subscreen, you can select your desired subscreen to make changes. The selected subscreen is outlined with white to differentiate it from the other subscreens.

Rename:	The **Rename** option allows you to change the name of the salvo/view once you have created it.
Remove:	You can delete a salvo/view from the list using the **Remove** button.
Reorder:	**Reorder** allows you to change the order of the salvos/views displayed. A new window pops up, which is where you drag them to change their order.

Current Video Wall

The **Current Video Wall** area displays the screen selected from the **Monitors** panel. You can add the screen using the grid configuration controls in the **Wall Designer** tab. In the **Wall Controller** tab, you can view subscreens with monitors displayed on them but cannot change the grid configuration.

©2021 Airship Industries

NEXUS CLIENT OPTIONS

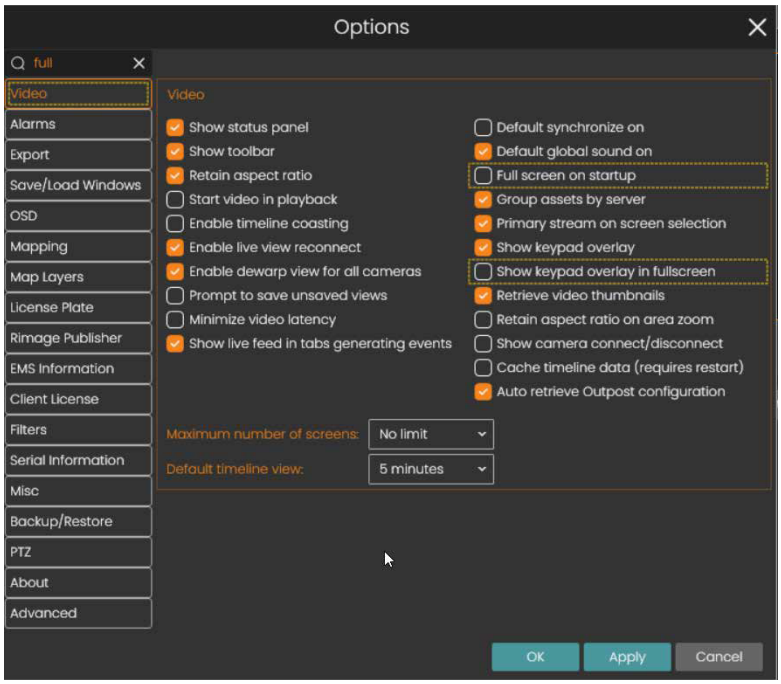
The **Options** menu allows the user to customize the **Nexus Client** to their needs. Users can change the default locations for saved clips and snapshots, modify quick-save time duration, login information, and video display properties.

The **Options** menu can be accessed by clicking on the  icon at the top right of **Nexus Client's** main window. In **Options**, you can scroll down through different submenus using the scroll bar at the right.

Video Options

The **Video** options submenu allows you to change settings for the display of cameras in the video tab.

📖 **NEW FEATURE:** Use the search bar at the top of the Options window to quickly find specific settings. Results will be highlighted in yellow.



The following settings will be applicable to all open video tabs as well as video tabs used in the future.

Show status panel: Check this box if you want to enable the status panel above each video screen. The status panel consists of settings for video recording, alarm ON/OFF, channel lock, presets, and display live view or playback.

Show toolbar: Check this box if you want to see the toolbar displayed in the Video tab.

Retain aspect ratio: When you select the **Retain aspect ratio** option, the video that Wall Driver displays will keep its native aspect ratio with any extra space being filled with black bars. When you do not select the **Retain aspect ratio option,** the video will be stretched to fit the available space in **Wall Driver**.

Start video in playback: Check this box to set all cameras' default mode to be "Playback", instead of "Live".

Enable timeline coasting: Check this box if you want the timeline in Timeline Tools to glide with momentum when you release the timeline in the same direction in which you dragged the timeline. It keeps moving unless you click on the timeline again.

Enable live view reconnect: Checking this box enables the client to reconnect live streams if/when they become disconnected.

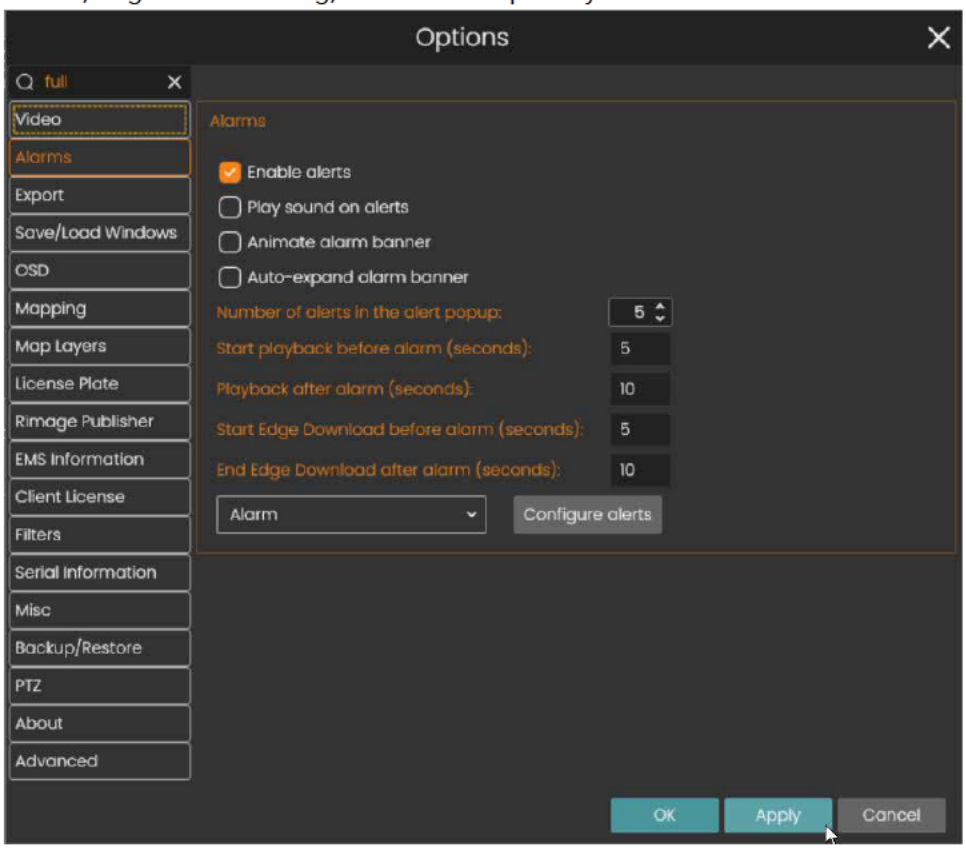
Enable dewarp view for all cameras: Checking this box enables fisheye Dewarp settings to appear below PTZ controls

Prompt to save unsaved views:	Check this box to be prompted to save newly configured view settings. By default, this is unchecked.
Minimize Video Latency:	Check this box to prioritize latency over frame rate.
Show live feed:	Uncheck this box to disable live feed in alarm tabs for alarm events when selecting an alarm event.
Maximum Number of Screens:	You can set a default value for a maximum number of screens a user can view at the same time. By default, the value is set to **No Limit.**
Default Timeline View	You can set the default time duration to display in the timeline bar in the Video tab. You can also change this value in **Timeline tools** in the Video tab, but you must set the default value here.
Default synchronize on:	Check this box to make video tabs be in Sync Play all the time. This will prevent viewing states from being in different states such as live or playback.
Default global sound on:	Check this box to turn on the sound by default.
Full Screen on Startup:	Check this box to open **Nexus Client** in full screen on your next login.
Group Assets by Server:	Displays assets under the associated Server. De-check if it is preferred to search and sort by camera name.
Primary Stream on Screen Select	Displays primary stream when the camera's screen is selected. Unselected screens display their secondary stream if configured in the Server Setup Tool.
Show Keypad Overlay:	Displays the keyboard shortcut used upon entry. The shortcut used will be displayed at the bottom of the **Nexus Client** window.
Show Keypad Overlay in Fullscreen	Displays the keyboard shortcut used upon entry. The shortcut used will be displayed across the bottom of the **Nexus Client** window while in fullscreen mode.
Retrieve Video Thumbnails	When this box is checked, Video Thumbnails will hover over the search bar as you scroll along the timeline.
Retain Aspect Ration on Area Zoom	Check this box to prevent the standard aspect ratio from altering the viewing panel due to the box drawn by the Area Zoom feature.
Show Camera Connect/Disconnet	Select this option to display connect or disconnect options when right clicking the camera from the assets list.
Cache timeline data:	Enable/disable timeline caching functionality. Restart required to take effect.
Auto retrieve Outpost camera configuration:	Check this box to automatically retrieve camera configuration from devices Outpost connected via Outpost.

©2021 Airship Industries

Alarms

Alarm recordings and motion detection are managed using **Nexus Client**. In this section, you may customize options for audible alerts, edge downloading, banners and priority level.

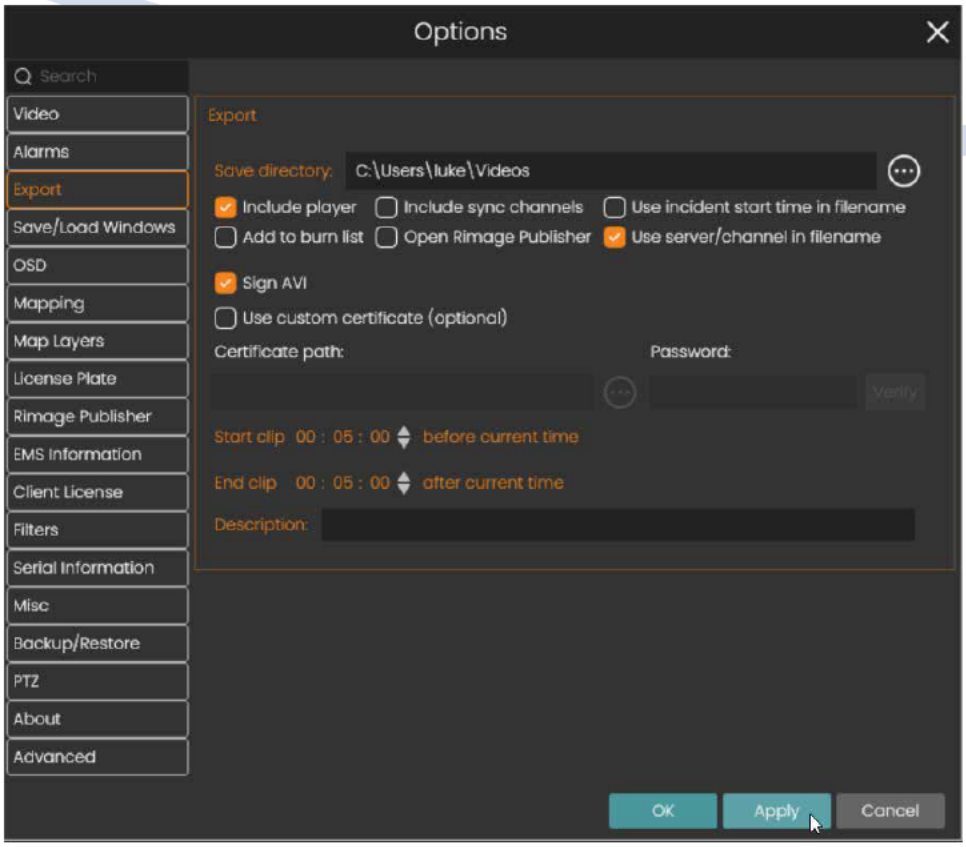


Enable Alerts:	Check this box to enable alarm notifications.
Play Sound on Alerts:	Check this box to enable sound for alerts.
Animate Alarm Banner:	Check this box to enable animations upon alarm trigger events. The Alarm tab must be open for the animation to appear.
Auto-expand Alarm Banner:	Check this box to automatically expand the Alarm Banner while alerting.
Number of alerts in the alert popup:	Set the limit for the number of alerts within the alert popup area.
Start Play back Before Alarm (s):	Choose the amount of time in seconds, prior to the alarm's trigger to start the alarm's video.
Playback after alarm:	Choose the amount of time in seconds, after the alarm's trigger to end the alarm's video.
Start Edge Download Before Alarm	Choose the amount of time in seconds, prior to the alarm's trigger to start downloading data to the Server from the Edge device.
End Edge Download After Alarm	Choose the amount of time in seconds, after the alarm's trigger to end downloading to the Server from the Edge device.
Configure Alerts:	Select the Alert type, then click Alarm Filter Options to set parameters.

📖 **Note:** To integrate alarm triggers with 3rd party monitoring systEMS, please see our *OnGuard Integration Guide*. Please contact Support for this document.

Export

Nexus Client provides the following default options for exporting footage which apply to all exported video.



Save directory:	Default directory to store exported clips.
Include player (save as .exe):	Check this box to save the player in addition to the exported .exe file upon each export.
Include sync channels:	If you have more than one subscreen and you want to add other channels in the export, select this option. If left unchecked, you will only export the camera screen that you have selected.
Use Incident Start Time in Filename	Check this box to add to the start time to the filename by default.
Add to Burn List:	If you select this option, it will send the selected video to **Nexus Client**'s burn list, which can be accessed by clicking "Burn CD". From the "Burn List" you can write your video to a disc.
Open Rimage Publisher:	Check this box to open the **Rimage Publisher** after you export the clip. Using the **Rimage Publisher**, you can write a large amount of video data to several discs using your Rimage System.
Sign AVI:	Check this box to append the video clip with a verification code at the end that prevents the tampering of the export video.
Use Custom Certificate:	You can use your own certificate key system to validate the export clip.
Certificate Path:	Enter the location of the certificate.
Password:	If using your own certificate key system, define the password to access the certificate.

©2021 Airship Industries

Verify: After you add the certificate, click this button to test the certificate and its password to make sure they are valid.

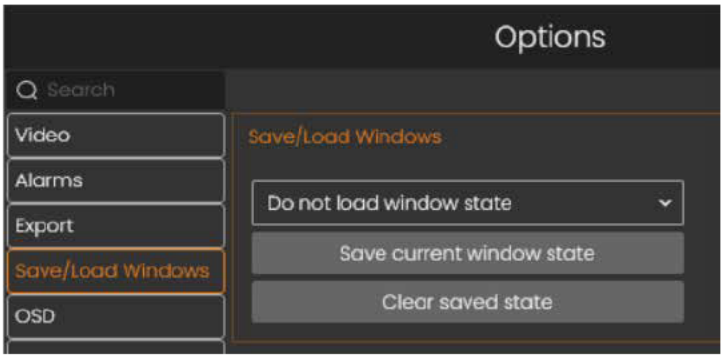
Start Clip: Amount of time to save before the current time to export the clip.

End Clip: Amount of time after the current time. The total clip time will also have the time for **Start Clip** and **End Clip**.

Description: You can always add some description for the clip for further use. You can further edit the description using "Detailed Export".

Save/Load Windows

One advanced feature that you should consider using with multiple windows is **Save/Load Windows**. This allows you to save the current content and window location when closing **Nexus Client**. It can open back to the same state the next time **Nexus Client** is launched.





Options:

Do not load window state: Select to not load previous Nexus Client window states upon the following login session.

Prompt to load window state on startup/login: Select this option to be prompted if you'd like to open the currently saved window state the next time you log in to **Nexus Client**.

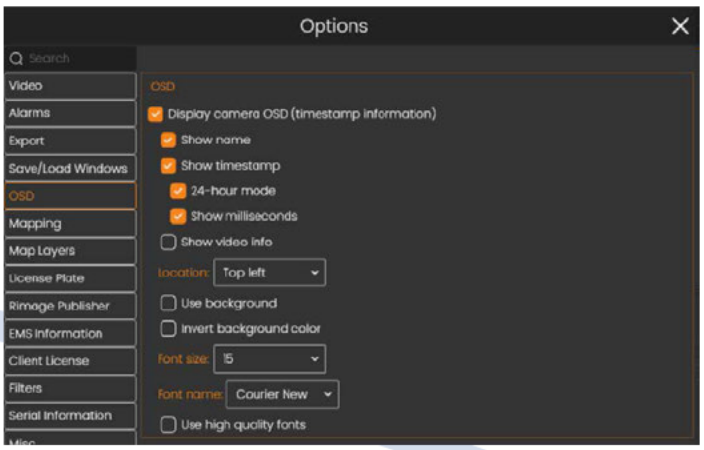
Load window state on startup/login: Check the box to be prompted if you would like to open the last saved window state when **Nexus Client** is launched.

Save Current Window State: Click this button if you want to save the current window state or overwrite an existing window state.

Clear Saved State: Click this button to remove the previously saved state.

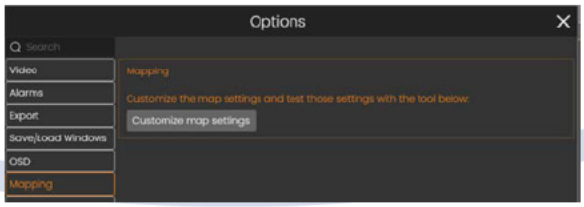
OSD

On-Screen Display options in the Settings Menu are provided by **Nexus Client**, agnostic to the device. The selected options apply for all video streams. On-screen display provided by the individual cameras will also display if enabled on the camera's settings. Check each box to enable its function, then click **OK** or **Apply**.

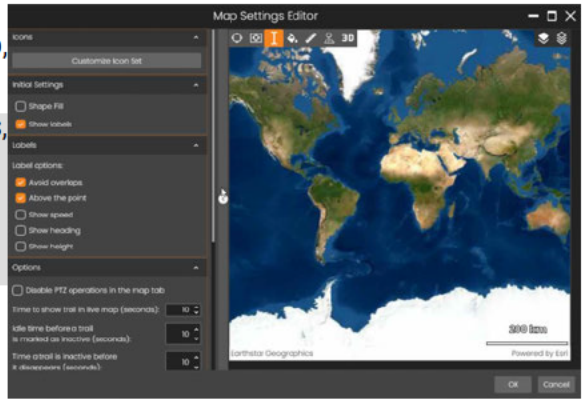


Mapping

From the Mapping submenu, click **Customize Map Settings** to open a tool that visualizes the changes in mapping display options. Changes represented in the visualizer apply to Nexus Client mapping tabs.



Select from Initial Settings, or click "**Customize Icon Set**" to edit the icons. Each box under Labels affects how labels appear on the map, check to enable the label feature.



📖 **NOTE**: The existing icon set for cameras, aerial objects, vehicles, people, and other icons may be replaced in the following folder: C:\Program Files\NexusClient\MapIcons\
Sub-folders separate each icon set. Images must be .png files to function. For best results, use a square image if replacing.

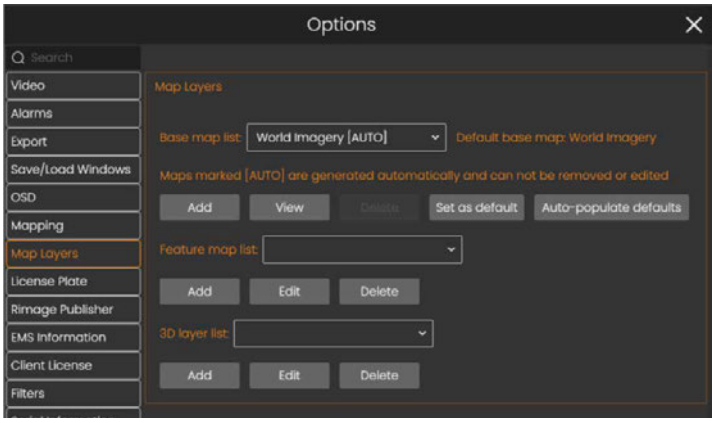
Disable PTZ Operations on map tab:	Disables PTZ control when viewing from the map search tab.
Time to show trail in live map:	Set the time in seconds to request location data from mobile devices.
Idle time before a trail is marked as inactive:	Set the time in seconds before inactivity marks a trail as inactive.
Time a trail is inactive before it disappears:	Set the time in seconds before inactivity removes the device marker.

Click the boxes under **Simulation** to simulate the movement and tracking of the available icons.

©2021 Airship Industries

Map Layers

Basemaps, layers, and 3D maps can be selected or added from the Map Layers submenu. Roads, trails, markers, locations, etc may be added as layers this way. Select Add, Edit or Delete to make entries or modifications to basemaps, layers or 3D maps. Some of the available options are outlined below.



Base Map List: The available map list options are available to select. Maps added will appear here.
Click Add to add new maps.

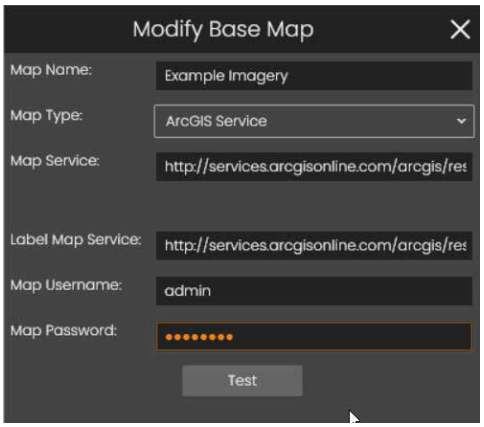


Use Basemap Service, File or Folder: Select the Service, File or Folder according to the Basemap used.

Map Name: Enter a custom name for the map or layer.

Map Type: Select from the default ArcGIS service, or select a file or folder.

Map Service: If using a Basemap file or folder, enter the file location in this field. For example, *C:\Program Files\NexusClient\basemapfile.tpk*.
Or, if using a service, enter the URL.



Label Map Service: Enter the URL, or file/folder location for the map label layer.

Map Username: Enter the **Username** associated with the login if using a Basemap Service.

Map Password: Enter the **Password** associated with the login if using a Basemap Service.

Set as default: Click this button to use the currently selected map as default.

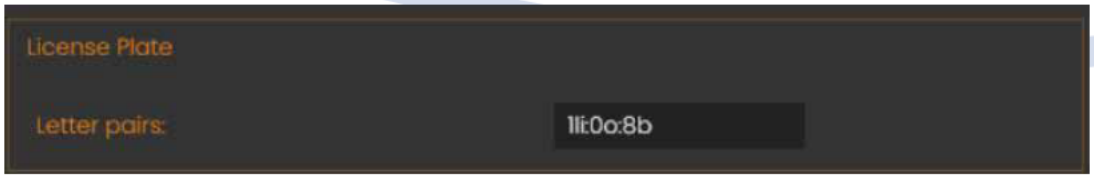
Autopopulate: Click this button to autopopulate the selected map when in the **Live Map** or **Map Search Tab**, instead of selecting the map on the top right of the map tab.

Feature Layer Database Path(.geodatabase): You can include various "feature layers" in your map. A "feature layer" shows specific areas/information of interest. Some example feature layers are: Police Station layer (shows all police stations in a particular area on your map), Fire Station layer, Traffic layer, etc. Enter the path to the feature layer database in this field or click "Browse" to use Windows File Explorer to help you find the path.

Feature Map List: Click Add to insert new feature maps as a geodatabase or service.

License Plate Options

Under **License Plate Options**, you can select the time recorded in milliseconds before a license plate gets detected. See the *ALPR Configuration Tool Guide* as well as the *ALPR User Manual* for complete setup instructions.

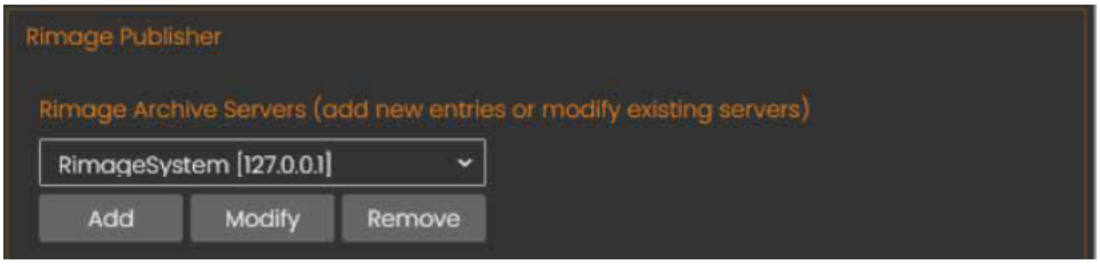


Start playback before detection (ms): Time before a license plate gets detected. Playback should start some time before the plate detection time so the video will include the vehicle moving across the field of view. This value is dependent primarily on the speed of the vehicle crossing the field of view of the camera. This value can be adjusted to improve review performance.

Letter Pairs Enter letters or digits that when read digitally, may appear as another letter or digit. I.e. if the number one appears as the letter L, or I, the software will recognize and pair results.

Rimage Publisher

The **Rimage Publisher** is an external backup tool which can digitally archive video data. You can add different Rimage Archive Servers by providing the name, IP address, and Port number of each server.

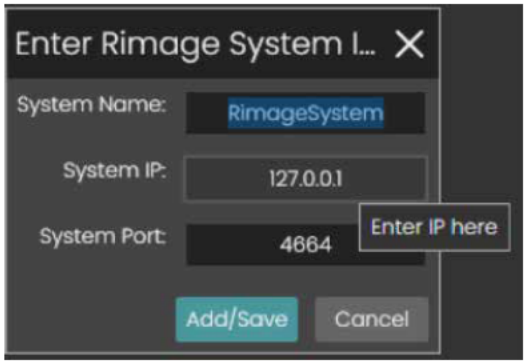


Select Server: You can select the server from the drop-down list once you have added at least one server.

Add: A new window pops up where you can enter the System Name, System IP, and System port number to add a new server.

Modify: Click this button to change the details of an existing server.

Remove: Click this button to remove an existing server.

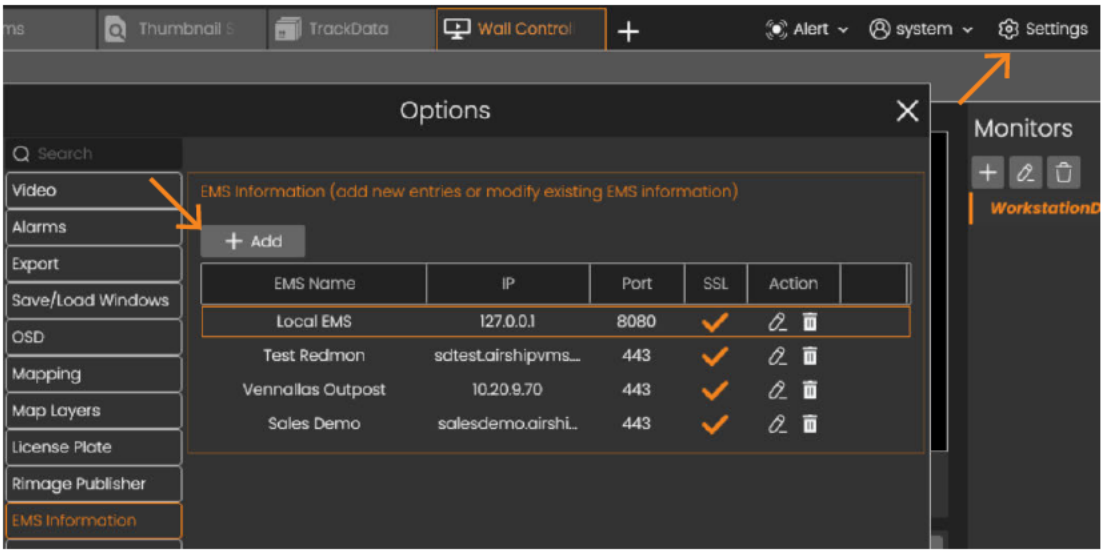


©2021 Airship Industries

Managed Mode

Users can access **Nexus Client** in either **Standalone Mode** or **Managed Mode**. In Managed Mode, **Nexus Client** is connected to a centralized system called the **Enterprise Management System (EMS)**. All user privileges can be controlled universally from the **EMS**. To add a new **EMS**, you simply enter the connection information of the new **EMS**. You can add multiple **EMS**'s if there are various organizations/locations that need access. All the **EMS**'s added are displayed in a drop-down in the login window where users can select the **EMS** they want to connect to upon login.

In order to access **Managed Mode**, the user has two options. One upon logging in, and another once logged in. The following steps show the user how to login from the **Nexus Home screen:**



1. From the **Nexus Home screen**, click the **Settings Wrench Icon**.
2. Select **EMS Information** from the left menu and select to Add, Edit or Modify a new or existing **EMS** entry.

Select EMS:	You can choose the **EMS** from the drop-down list if you have already added one.
Add:	Click this button to add a new **EMS**. See "Adding a New EMS" covered on page 56.
Modify:	You can change the details of any existing **EMS** using this option.
Remove:	Click this button to remove the **EMS**..

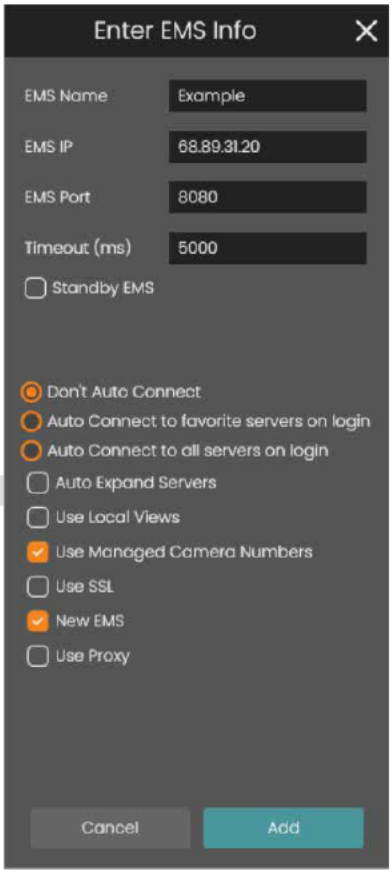
3. The user can also edit **EMS Information** from the **Nexus Log In Screen** (see next page).

Adding a New EMS

Adding a new **EMS** entry can expedite a user's need to access other servers.

If the user does not have a **Managed Mode EMS** IP Address, the following steps can be used to create one:

1. Click the **Edit Button** to the right of the **EMS drop-down menu**, or, click **Add** under **Managed Mode**.
2. The **Enter EMS Info** box will pop up.
3. Creating a new **EMS** will require completing the following steps (all steps for creating a new **EMS** are highlighted in the image above with four arrows):



EMS Name: Name of the **EMS**. Choose a name that makes this **EMS** easy to identify in other areas of the Airship ecosystem.

EMS IP: IP address of the **EMS**.

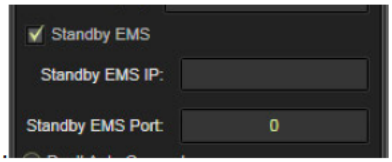
EMS Port: Port Number the **EMS** is listening on. Default value for the web port is 80 but make sure that the **EMS** network port value matches with this value.

Timeout (ms): This value sets the amount of time that **Nexus Client** waits to hear back from this **EMS** before considering it unreachable. Default value for the web service timeout is 5000ms.

📖 **IMPORTANT:** A user can also create a standby **EMS**. Seen below.

Standby EMS: Select this option to set up a backup **EMS**. If the primary **EMS** connection fails upon login, the user can refresh the session, which will attempt to connect to the Standby **EMS**.

1. Click the box to the left of **Standby** EMS.
2. Insert the **Standby EMS IP** information and click **Add/Save**.



©2021 Airship Industries

Modify an Existing EMS

Modifying can expedite a user's need to improve an existing **EMS**. Click the edit button next to the EMS listing.

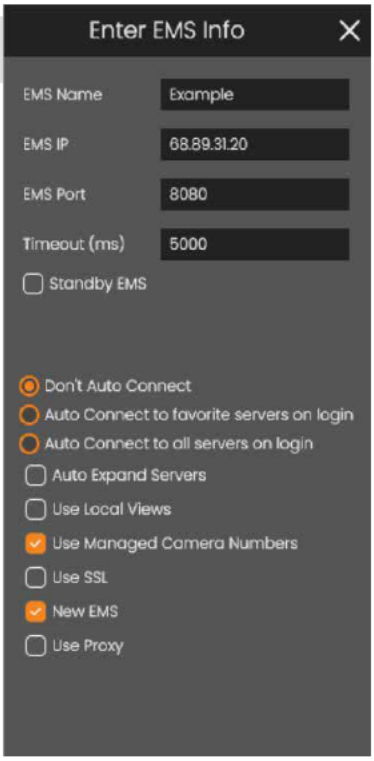
An existing **EMS** can be modified by altering the options within the red border seen below. Click the **Add/Save** button when done with modification.

Don't Auto Connect: Select this option to prevent automatically logging in to an **EMS**.

Auto Connect to Favorite Servers on Login: Select this option to login with a preferred **EMS**.

Auto-connect to all Servers on Login: Select this option to automatically connect to **EMS** servers when you log in to **Nexus Client**.

📖 **WARNING!** Do not use the option above if you have a large number of servers but only use a few at any given time.



Use Local Views: Enabling this option will revert to save/use views on a user's local PC on which **Nexus Client** is running instead of using the "Shared Views" saved to this **EMS**.

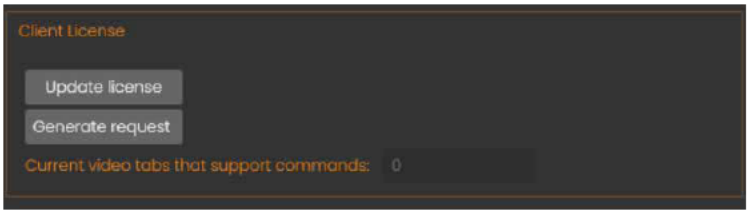
Use Managed Camera Numbers: Check this box to use camera numbers from the manager (**EMS**) instead of the camera prefixes.

Use SSL: Enable this option to use SSL for a more secure connection between **Nexus Client** and this **EMS**.

Use Proxy: Enable this option to connect to other servers.

Nexus Client License

Nexus Client needs a valid license to enable the Wall Driver emulation functionality in it. Contact the Airship Support team to generate a new license.

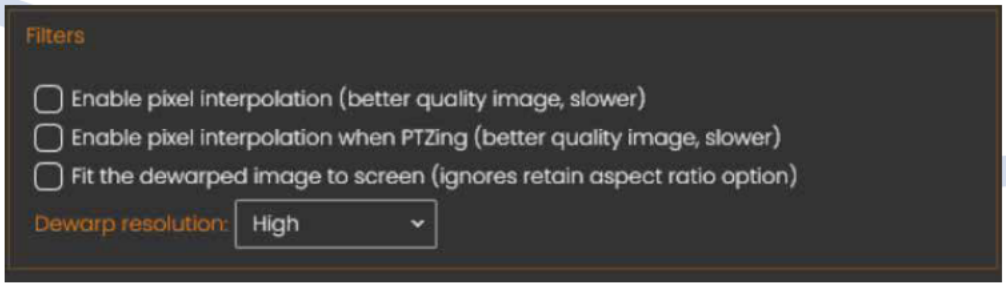


Generate Request: Click this button if you wish to create a new license. You have to send your 'License request.dat' file to Airship Support to process your request. They generate the license and send you back a "license.dat" file which you will use to properly license your **Nexus Client**.

Update License: Once you receive the license.dat file from the Support team, click this button to update.

Current Video Tabs that support commands: Value for a maximum number of video tabs that support commands from the Wall Drivers.

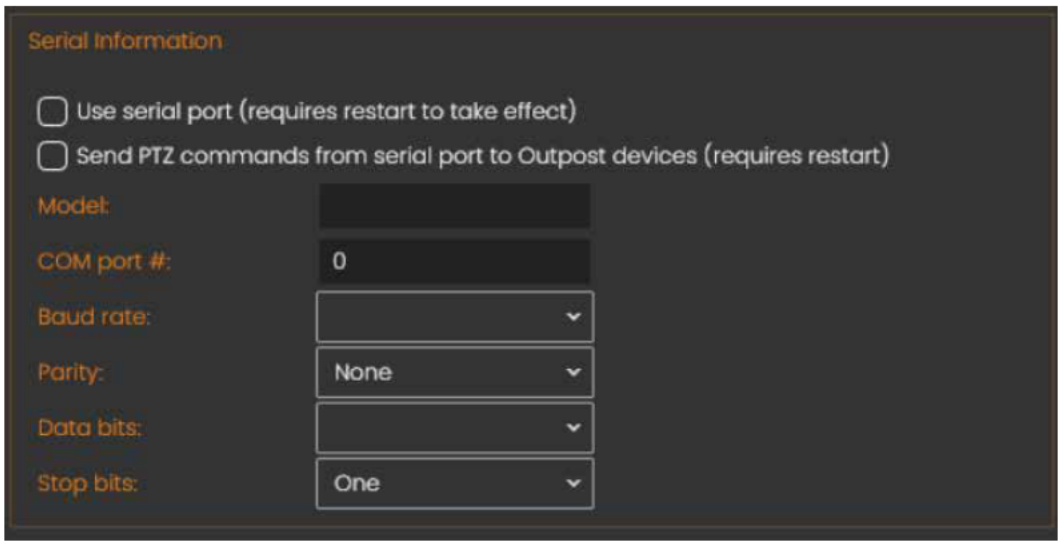
Filters



Enable Pixel Interpolation:	Click to enable pixel Interpolation, which prioritizes image quality over frame rate.
Enable Pixel Interpolation when PTZing:	Click to enable Pixel Interpolation when Panning, Tilting, or Zooming
Fit the dewarped image to screen:	Checking this box ignores the selected aspect ratio options.
Dewarp Resolution:	Toggle global resolution settings for fisheye cameras.

Serial Information

Nexus Client allows you to connect third-party devices to Airship Server using a serial interface. These devices can be used to activate a set of cameras on individual monitors under pre-determined circumstances via the Pelco keypad protocol. For example, a Fire Alarm system might connect through the Serial Interface to launch cameras near the fire to an active monitor.



Use Serial Port:	Check this box to connect the camera to the serial port. You have to restart **Nexus Client** to make these changes take effect. All other information such as model, com, baud rate, parity, data bits, and stop bits should be provided in the documentation of the device.
Send PTZ Commands from Serial Port to Outpost Devices:	Remote Outpost devices connected can also PTZ by serial connection, by checking this box. Restart is required upon selection.

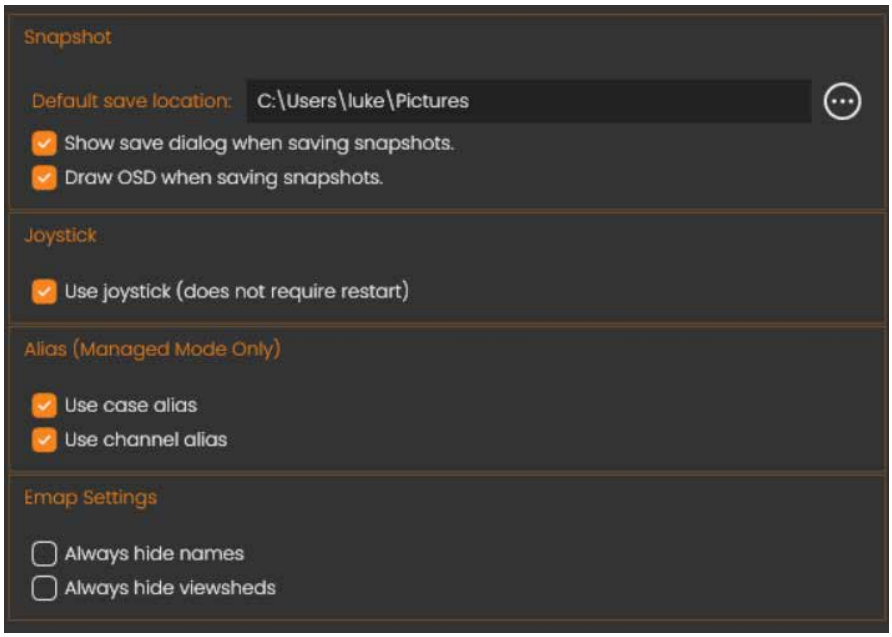
📖 **IMPORTANT:** Contact Airship Support for more information about these devices.

©2021 Airship Industries

Misc

Snapshot

Snapshot takes the current image file from the video and saves it to a particular directory on your workstation for future retrieval. It also provides you with the option to change the default save location.



Default save location:	You can set the default location to which you want to save snapshots.
Show save dialog when saving snapshots:	Checking this box will open a file explorer every time you take a snapshot. Do not select this box if you want to save the snapshots in the default location without re-confirmation.
Draw OSD when saving snapshots	Retains the information displayed on screen when saving screenshots.

Joystick

Select the check box to use an **Airship Joystick**. This allows **Nexus Client** to control movement on RS-232 connected joysticks. Contact Support for further hardware details.

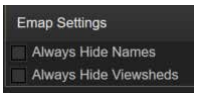
Alias

Each channel on a device has a device name and an alias, similar to cases. All channels/cases on any server that has ever assigned the channel/case will reflect the new alias name. This includes both active assigned, and inactive channels.

Use Case Alias:	The camera entry will use the Case Alias by default.
Use Channel Alias:	The camera entry will use the Channel Alias by default.

Emap

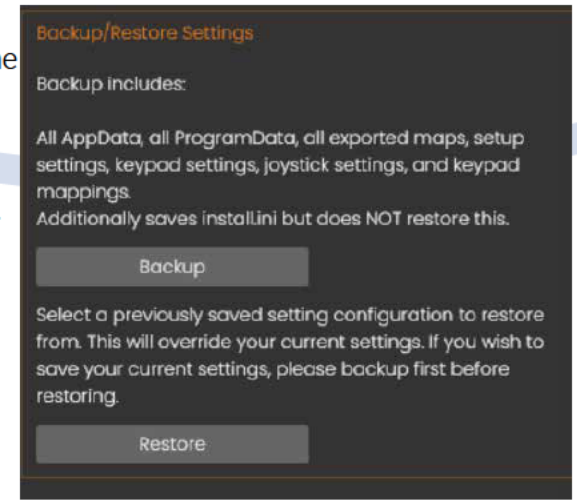
While using the Emap tab, icons may display or hide names and viewsheds. To always Hide Names or viewsheds, check the associated box.



Backup/Restore

Select **Backup** to store all AppData, ProgramData, exported maps, setup, joystick, keypad settings and mappings. Backup also saves the install.ini file.

Select **Restore** to load a previously saved backup. This will override current settings. Use **Backup** to save settings prior to restoring data.



PTZ

Click the drop-down selection under On-screen PTZ to choose from the available color options, then click **Apply**. By default, Enable Directional PTZ and the Enable area zoom and click to center function are Enabled. Uncheck to disable these functions if you have no need for on-screen PTZ options.

Click **Configure PTZ Pane** to select which functions appear in the PTZ pane in live view.



About

The **About** section displays the current version of your **Nexus Client**.

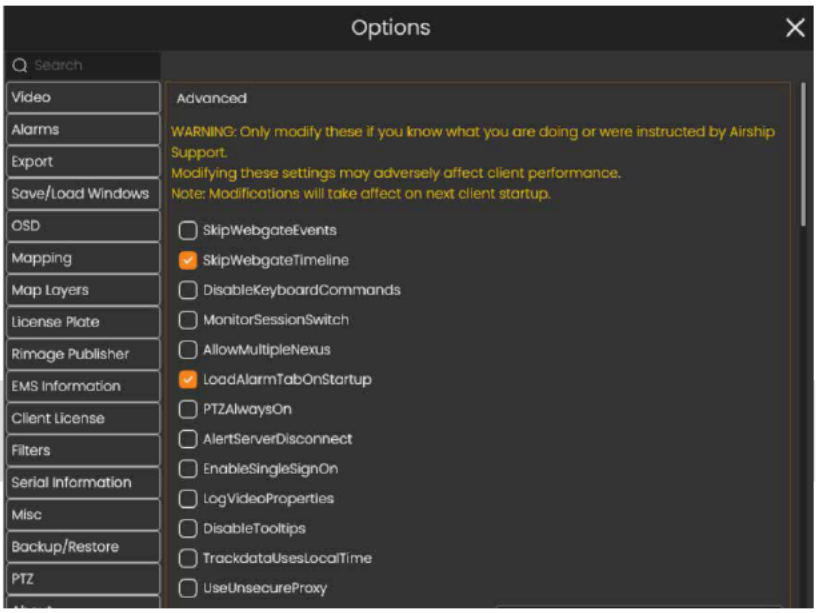


©2021 Airship Industries

Advanced

The Advanced menu is reserved for configuration aided by an Airship Support Agent. Modifying the settings found in this section may inadvertantly affect or impede performance.

Using the mouse to hover over each item will reveal a tool tip that briefly details the selection, however, please contact an Airship agent for further information on making changes within the Advanced section.



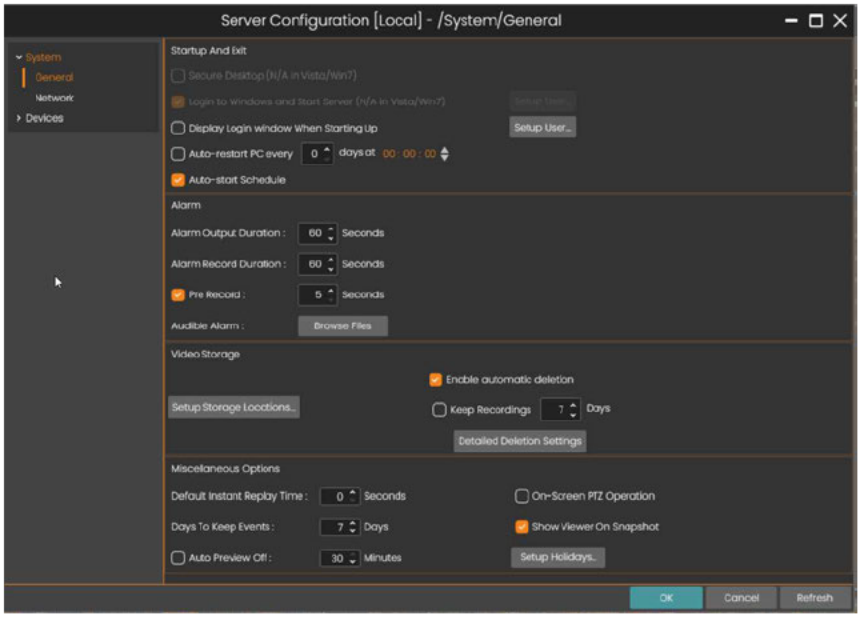
📖 **NOTE:** Use the Search feature to find things quickly.

Configure Server Settings through Nexus Client

Using **Nexus Client**, users with necessary permissions can access server configurations using the Configure button to the far right of each server in the **Servers** tab.



1. Open the **Servers** tab if it already exists or click the ➕ button at the top of the main window to open a new tab, and then select **Servers**.
2. The **Servers** tab displays all the servers in **Nexus Client**.
3. Select a server to view its configuration options. Note that only users with valid permissions can access server settings.
4. Click the **Configure** button. The **Server Configuration** window appears with a menu on the left and expandable sections showing submenus. Clicking on these submenu options will show information to the right.
5. A user can save, cancel, or apply the changes using **OK**, **Cancel,** or **Refresh**, respectively, at the bottom of the window.



📖 When you hit **OK**, a warning message appears saying the server will restart. Click **Yes** to restart the server.

General

Startup and Exit

Display login window when starting up: Checking this box will open a login window every time you open the Airship Server application. Uncheck this box to login with the default username and password, which can be set using the **Setup User** option.

🕮 The option above only applies when you are not using Server as a service.

Setup User: You can see this option only when **Display login window when starting up** is not checked. You can provide the default username and password using **Setup User**.

Auto-Restart PC every: **Auto-Restart** is useful for ensuring system stability and for coordinating with other system administration events. You can provide a value for a number of days between each system restart and set the exact time for which you want the restart to occur.

Auto-Start Schedule: This option sets the recording schedule to be automatically enabled after system startup.

Alarm

Alarm Output Duration: This option defines how long an alarm condition lasts once triggered, which affects the duration for which you can hear **Audible Alarms** and trip **Relays**.

🕮 A new alarm condition cannot start on the same channel or sensor until the existing one ends.

Alarm Record Duration: A video recording initiated by an alarm will record video for a specified amount of time, which you can enter here.

Pre-Record: Video recording will start recording with the lead time as a buffer. Define this time here.

Audible Alarm: This option allows you to add your audio file to play for an alarm.

🕮 Users running Server as a service do not require the above option.

Video Storage

Enable Automatic Deletion: Check this box to delete old recordings automatically when the storage locations run out of space. Enabling this option ensures that there is always space available for the most recent recordings.

Keep Recordings (Days): You can store all video recordings for a maximum time length defined in this field. If recording goes beyond the time limit, a new file will be started without missing any video information.

🕮 If there is not enough space for the specified number of days, the server will remove the oldest recording, giving more space to the new recordings coming in.

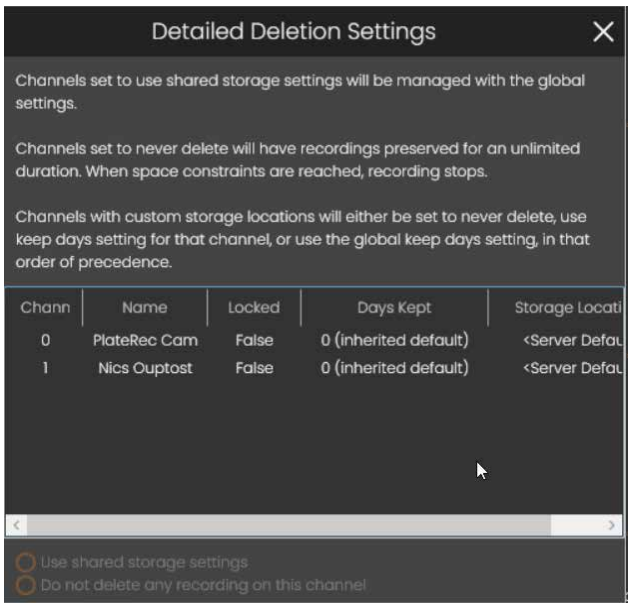
Setup Storage Locations: This option will allow the user to add a new destination for the files on the selected channel. If not selected, all the data will be stored in the default location.

🕮 Set Storage Locations and Set Default Storage are only available when you select a channel.

©2021 Airship Industries

Detailed Deletion Settings:

Detailed deletion settings will provide the administrator more options to select for each camera on the server for deletion. Clicking this button will open a window listing all available cameras on the server.



Use shared storage settings:

As shown in the above screenshot, a user can view the detailed information for all the server's cameras such as: camera name, lock status, number of days kept, and storage location. Select a camera to perform different actions on it.

The user can set specific channels to use shared storage settings.

Do not delete any recordings on this channel:

Channels set to never remove any recordings will have recordings preserved for an unlimited amount of time. Typically, this setting is set in conjunction with the **Set Storage Locations** option that records to a different storage location with an alternative mechanism (offloads the recordings from other channels). Otherwise, the shared storage location will eventually fill up completely.

Keep __ days of recording:

Select the number of days you would like to keep recordings before they are deleted.

Set Default Storage:

This option is a toggle to switch back to using the shared storage instead of a custom storage location for the currently selected channel.

Set Up Storage Locations:

Set up a custom storage location for the currently selected channel.

Miscellaneous Options

Default Instant Replay Time:	Set the instant replay time at the start of each session. Minimum is 5, and maximum is 300.
Days to Keep Events	Set the number of days to retain events on the Server.
Auto Preview Off:	This option, when selected, will turn off the preview automatically and will lock the Server application after the specified number of minutes of inactivity.
On-Screen PTZ Operation:	This option allows you to control the PTZ camera's movement on the main GUI screen using your mouse.
Show Viewer on Snapshot:	This option opens the snapshot viewer when you take a picture.

🕮 All the options above do not apply if you are using Server as a service.

Setup Holidays:	The user can manage holidays here for camera and sensor scheduling. This function will disable recording for the selected day.

Network

The **Network** submenu allows the user to enable/disable various remote access functions such as clients. Also, you can change various ports used by the Remote Clients and Web Clients. A change to port values here will require a change to the default port setting on the Remote and Web Clients.

🕮 We recommend users not use the default ports for security reasons. It is important to copy the port settings and keep them written down outside the Network tab.

Network Administrators should be made aware of the ports required for client to server communications. They should update the router configurations if they change the ports. Care should be taken to avoid port conflicts with other software on the server and clients.

Remote Client Service

Remote Client Service:	Check this box to enable remote access to the server.
Check Users:	Check this box to validate client access to the server's user list and authentication rights.
Multicast IP Address:	Enter an address to which you want to send multicast data to multicast capable clients.
Max Bandwidth Used:	This setting governs total bit rate the server is allowed to use in servicing all clients. A value of 0 indicates that the bit rate is unlimited while a value of 32000 means that the bit rate is 32kbps.
Command Port:	The port used to connect to Airship Server, the default is 6001..
Video Stream Port:	The port used for live video streams.
Remote Replay Port:	Network Administrator changes port numbers here.
Remote Replay Data Port:	Network administrator can change port numbers here. Make sure to change the value for both server as well as client.

©2021 Airship Industries

Web Service

Check this box to enable Web Client access on this server, and add the associated Server port.

> 🕮 When you select the Web Service option, you can see Limit one channel per user and Server port options. This is helpful for particular system functionalities like video portal in the absence of Transcoder and ALPR.

SSL Settings

Remote Certificate Path:	Displays path to chosen certificate. Click “Browse” to select a location for the certificate.
Remote Key Path:	Certificate key component. Click “Browse” to choose a location for the key.
SSL Password:	Password to file that holds a certificate.
SSL Command Port:	Enter the command port number.
SSL Playback Port:	Enter the playback port number.
SSL Preview Data Port:	Enter the preview data port number.
SSL Playback Data Port:	Enter the playback data port number.

E-mail

SMTP Server and email information are used for the Send Email option in the server configuration under Devices > Cameras > [camera name] > Alarms > Custom Alarms.

SMTP Server:	Enter the hostname/IP address of your SMTP Mail Server. Your network administrator can provide this information.
Port:	Default port for SMTP connection is 25.
Return E-mail Address:	Enter the address from which emails will be sent.
To:	Enter the email address where you would like all alarm emails to be sent. > 🕮 Note that all alerts will be sent to this email address. To select individual alarms, enable notifications in the user settings in **EMS** (or **Airship Server** if unmanaged).
Server Requires Authentication:	Check this box if you want SMTP Server to authenticate the sent emails that require SMTP login.
Setup SMTP Login User:	Click this button to provide username and password for SMTP login.
Test:	Sends a test email using the information provided to verify the settings are correct.
Default:	Click this button to reset all network settings back to the default values.

Devices

The **Devices** submenu provides the list of all available cameras on the server along with the camera type of either analog or IP cameras.

Add a Camera

> 🕮 **NOTE:** This option is only available for standalone **Airship Servers** with server-side camera management.

Click the **Add** button to add an analog or IP camera by providing information such as IP address and port number.

Device Name:	Name of the device.
Device Type:	Select the device type from the drop-down list.
Device IP:	IP address of the device.
Device Port:	Default port number of the device. Typically, the value is 80.
Username:	Username to connect to the camera.
Password:	Password to connect to the camera.
Timeout:	After the specified value for timeout, the server will stop trying to connect to the camera. Default value is 10000ms = 10 seconds.
Secondary Device IP:	When a camera's primary IP goes down, the camera may optionally fail over to a secondary IP. Airship Server will periodically check if the primary IP is available, and switch back when it becomes available again.
Secondary Device Port:	Enter the port number for the device's secondary IP.
RTP over RTSP:	If checked, TCP is used to connect to the device, and if unchecked, UDP is used.
Retrieve Camera Data:	Retrieves camera data such as connected servers and encoders.
Bandwidth Saving Mode:	If **Bandwidth Saving Mode** is checked, **Nexus Client** will try to minimize the bandwidth utilization. It will disable the video stream until an alarm comes in, and then connects to the stream at the frame rate that was previously set.
Server Motion Detection:	Check this box for the server to handle the motion detection rather than the camera or the encoder.

> 🕮 **Bandwidth Saving Mode** and **Server Motion Detection** cannot be enabled concurrently because **Server Motion Detection** requires a continuous live stream which will be disabled if **Bandwidth Saving Mode** is enabled.

Use Edge Recording:	When streaming bandwidth is limited, check this box to store footage directly at the edge device and retrieve selected footage on demand.
Use Client OSD:	Check this box to enable Nexus Client's on-screen display.

- Deleting a device is a simple task as you can select the device from the list of devices and click the **Delete** button to remove it from the server.
- In the same way, you can modify the information regarding any camera by simply selecting the device name and clicking the **Modify** button.

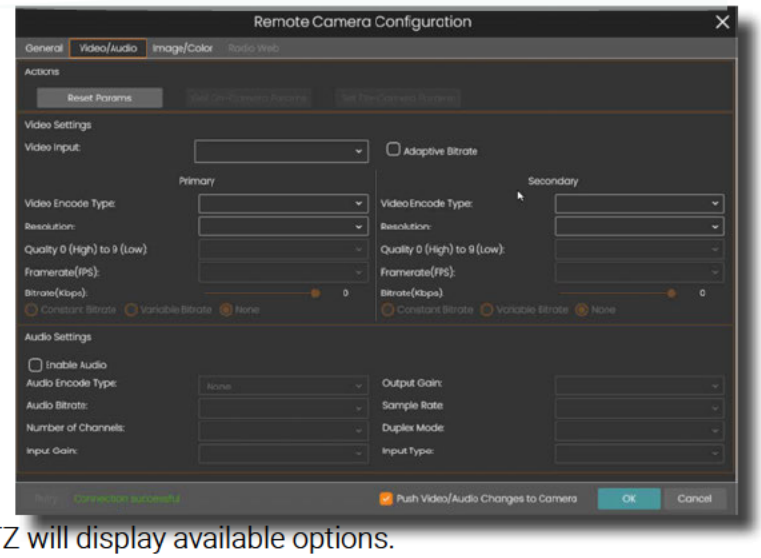
©2021 Airship Industries

Configure a Camera

Configuration will fetch the detailed information about the camera and provides options to change the camera's video/audio settings.

📖 The configured camera is the camera selected on the left-hand side under **Devices**. Changes made to video parameters apply to all channels on a multi-channel IP device.





General: Device information is displayed as well as the IP address.

Video/Audio: Current Video and Audio settings available for the selected device are configurable based upon the options native to the device.

Image/Color: Image settings which are available to the device are displayed for configuration. Note that the available settings vary by device.

Digital PTZ: Cameras that support Digital PTZ will display available options.

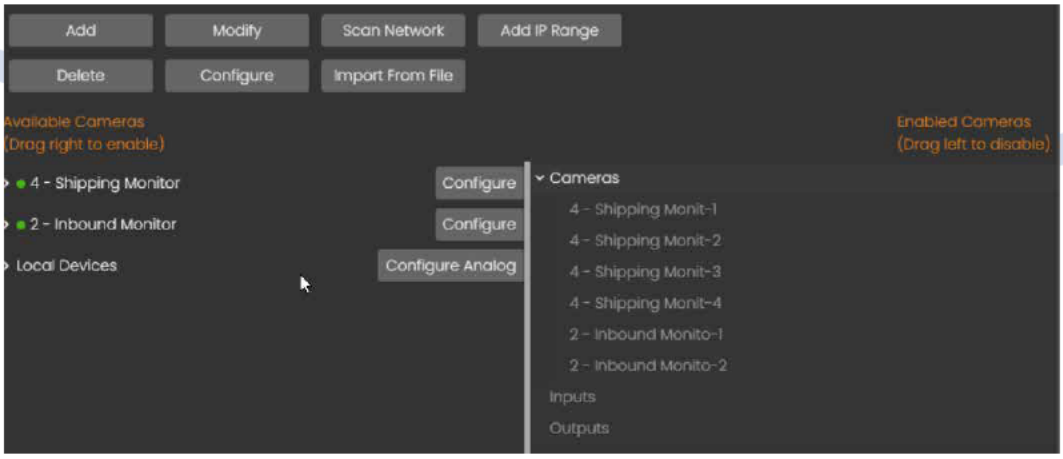
Area of Interest: Cameras with Area of Interest options available will prioritize stream quality within the selected area. Without an area of interest area set, the full image will be prioritized equally.

Radio Web: Devices such as PTT radios with web-based user interfaces will be displayed for configuration.

Add Multiple Cameras

A user can add multiple cameras at a time using three different modes. When you select a mode, you can see a description given below in the same window.

- Scan the Network
- Import from File
- Add IP Range



Scan the Network

Click this button to scan the network which will display any available cameras on the network. The user can add the needed cameras by selecting them. The server will use several standard mechanisms to attempt to detect the valid IP devices on the local area network.

Import from File

Click this button to import a list of cameras from a file that is stored locally on your machine. You simply need to choose the path of the folder from which to import the file.

Add IP Range

The user can also add multiple cameras by providing an IP range. Provide the start and end IP addresses along with the port numbers to search for the IP addresses. The user can also provide the device type along with a username and password for that device.

©2021 Airship Industries

Cameras

The **Cameras** submenu will display all the available cameras on the server. The overview provided shows some basic settings. Click a camera to see its detailed configuration information.

Display

The **Display** screen shows the current view of the camera selected on the left, along with different configuration options.

Relocating On-Screen Display (OSD) text:	Check to enable this option. Move the On-Screen Display text blocks anywhere on the channel display. Click the camera name or date/time to move them.
Camera Name:	You can enter a camera name, which will be shown on the On-Screen Display (OSD) and at various places throughout the Server and Client displays.
Display Camera Name:	Check this box to display the camera name on the OSD.
Date Format:	Configure the date format for the OSD.
Display Date and Time:	Check this box to see the server date/time on the OSD.
Video Format:	Select NTSC/PAL, depending on the camera type.
High Contrast Overlay:	Check this box to see OSD font easily in various scenarios.

Privacy mask

Enable Privacy Masks:	By checking this box, you can use the mouse to draw one or more squares on the video screen to hide certain areas from viewing. Right-click on a mask to remove it.
Clear All:	Removes all masks from the camera.

Dual Stream

📖 **IMPORTANT:** This section is only displayed if an analog camera is selected, and requires a secondary stream to be selected within the **Server Setup Tool**.

Enable Dual Stream:	If checked, Remote Clients will see this camera using a live stream.
Resolution:	Set the screen resolution or detail level.
Frame Rate:	Enter the desired frame rate of the video stream.
Quality:	Set the compression quality. Higher quality uses more network and decoding resources on the client.
Stream Limit:	Check this box to force a maximum network bandwidth usage for the stream.
Default:	Returns all settings to default values in this tab.
Copy To:	Using this button, you can copy the current camera settings tab to other cameras. Use it carefully, as you can replace one camera's settings with incorrect ones.

Color

The **Color** tab allows changing the channel's brightness, contrast, hue, and saturation settings. This function allows the user to automatically adjust for environmental lighting changes at night or during the day, or for other situations such as exterior lighting timers.

Brightness:	Makes the image brighter or darker.
Contrast:	Helps you control contrast between dark and light.
Saturation:	Saturation control for more or less vibrant colors.
Hue:	Controls color hue correction, such as adjusting for fluorescent lighting.
Default:	Returns all settings to default values in this tab.
Toggle Schedule:	Opens a window with an advanced **Color Schedule** panel. Once opened, you can hide it using the same button.

Toggle Schedule

The advanced color schedule allows you to record changes in the color settings at any time of the day. You can increase the brightness and saturation for night time outdoors, or reduce the contrast to make shadows clearer in bright daylight.

Color Name:	Enter a name to describe the purpose of your color time settings.
Start Time:	Enter the start time for the color settings to take effect.
Add:	Adds a specified time frame to the schedule.
Delete:	Deletes the time frame selected for the schedule.
Modify:	Edits the saturation, contrast, hue, and brightness settings for the time selected in the schedule.

🕮 A **Color Schedule** time frame may not start before midnight and end after midnight. To approximate this, we have the time frames end right at midnight and a matching color scheme start right at 00:00:01 AM; 24HR time.

🕮 Extreme values in any of the color settings can result in 'noisier' video, increasing the size of resulting video files and potentially reducing the amount of video a server can store. If your color changes cause more noise in the live stream, back off on the changes until you get a good balance between video clarity and minimal noise in the video image.

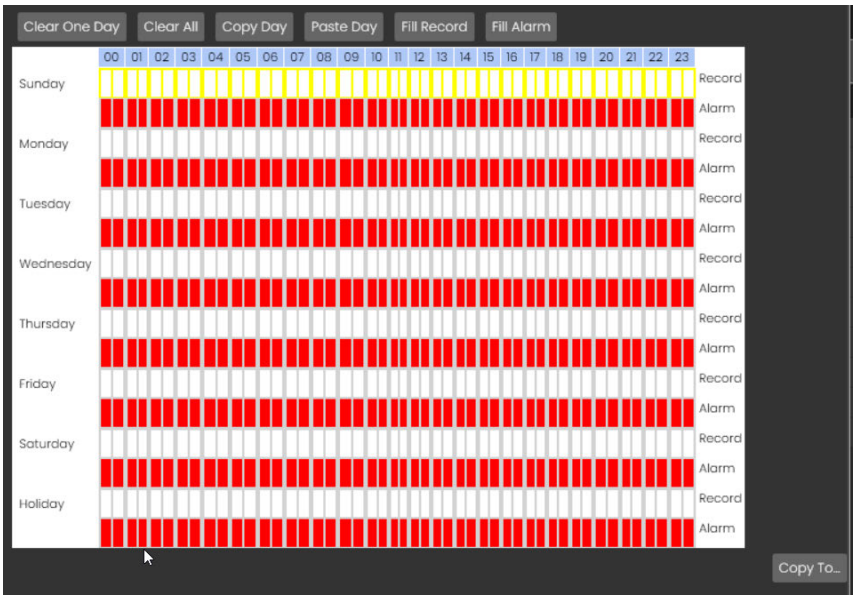
🕮 If a **Color Schedule** ends without another time frame right afterward, that camera will revert to the settings in the main **Color** setting above.

Copy To:	Using this button, you can copy the current camera settings tab to other cameras. Use it carefully, as you can replace one camera's settings with incorrect ones.

©2021 Airship Industries

Video and Schedule

The **Weekly Calendar** lists each day of the week, including holidays. See the Setup Holidays option in the **General** tab. In the example screenshot below, hours of each day (split into two rows) are listed at the top; one for constant recording, and the other for alarm recording. Alarm recording activates alarm detection, resulting in recordings when an alarm occurs on the camera for the specified time period.



Click the day/time grid to draw a line representing schedule time period. Standard recording is in blue, and alarm is in red. For a selected time period, right-click to see more options.

Clear One Day:	Clears the currently selected day of the week, Record and Alarm.
Clear All:	Clear all will completely remove recording of any kind for the whole week.
Copy Day:	Duplicates the currently selected day of the week to be used elsewhere.
Paste Day:	Pastes the previously copied day of the week into the currently selected day.
Fill Record:	Populates all Recording slots in the schedule.
Fill Alarm:	Populates all Alarm slots in the schedule.
Copy To:	Using this button, you can copy the current camera settings tab to other cameras. Use it carefully, as you can replace one camera settings with incorrect ones.

PTZ

The **PTZ** (Pan-Tilt-Zoom) configuration tab allows the user to enter the configuration details for any PTZ cameras connected to the server.

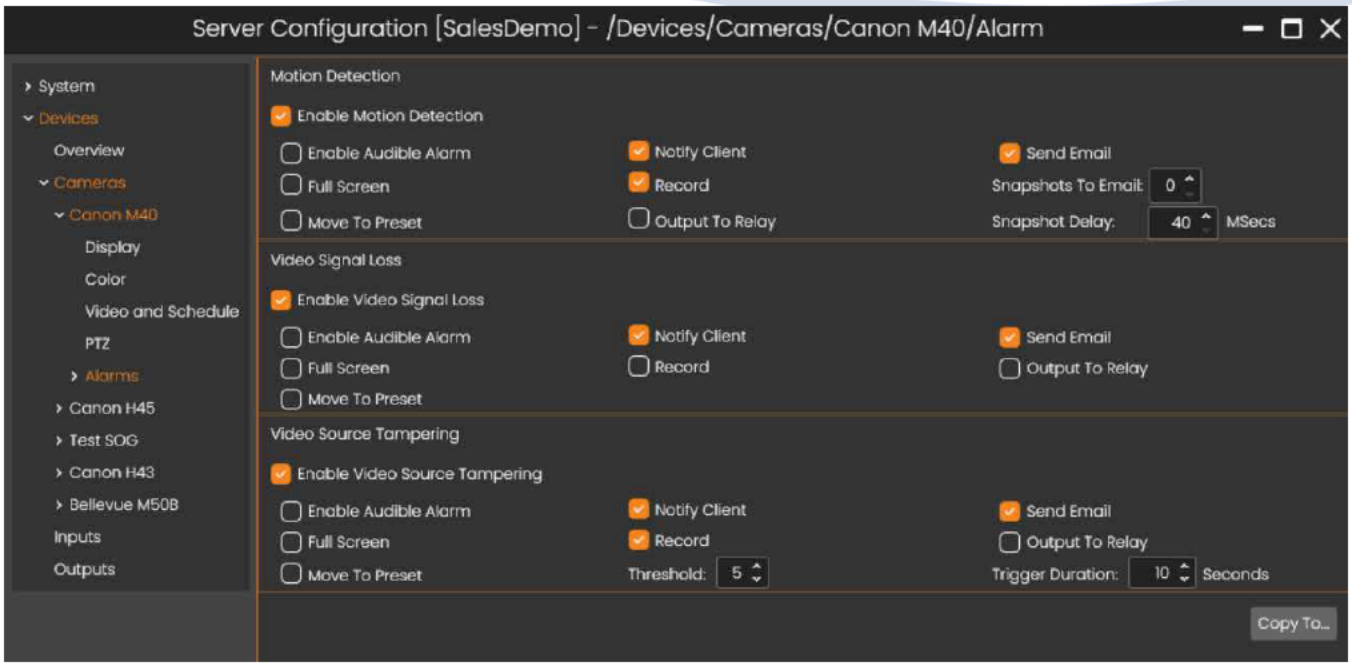
🕮 Refer to the camera manufacturer's documentation for the appropriate values.

PTZ Protocol:	Select the correct protocol for use with this camera.
COM Port:	Select the COM port to connect the PTZ control.
Baud Rate:	Select the baud rate.
Address:	Select the right RS-485 address for the camera.

Alarms

Global alarm settings are required to enable a variety of functions concerning alarms throughout the system, from PTZ presets to schedules and more. All settings are actions to perform upon an alarm trigger.

> 🕮 Alarm functions can be set on a single channel using the "Custom Alarms" feature, providing more flexibility and innovative sensor/alarm/recording combination.



Motion Detection, Video Signal Loss, & Video Source Tampering Alert Options

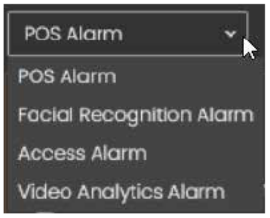
The following notification options are available for motion detection alarm events per camera selected.

Enable Motion Detection	Click to enable motion detection alarm events for the selected camera.
Enable Audible Alarm	Click to enable an audible alarm for when motion events occur on the selected camera.
Full Screen:	Causes the camera on which the alarm occurred to go into full screen upon alarm-trigger.
Move to Preset:	Causes camera to use its PTZ functionality to move to a specified preset upon alarm.
Notify Client:	Sends a message to any clients currently connected to this camera when an alarm is triggered.
Record:	Causes the alarm condition to result in recordings captured for the channels specified in alarms > Alarms Record Duration. The default value is the same camera number for which you have configured the current settings.
Output to Relay:	Causes alarm to output to previously set up Relay(s).
Send Email:	Enables the sending of an email when an alarm is triggered.
Snapshot to Email:	Attaches the desired number of snapshots from the footage associated with the alarm event.
Snapshot Delay:	Sets the start time of snapshots selected from alarm event footage.

©2021 Airship Industries

Custom Alarms

The alarm system has four alarm triggers. Each trigger option may perform different actions according to the settings used below. Select POS, Facial Recognition, Access, or Video Analytics alarm to apply a custom setting.



Enable Alarm: Check this box to enable the alarm trigger.

Enable Audible Alarm: Emits an alarm sound through the speakers connected to the server. Refer to the Alarms section for more info on audible alarms. The Alarms tab must be open.

📖 **Note:** Running Server as a service does not require the above option.

Full Screen: Causes the camera on which the alarm occurred to go into full screen upon alarm-trigger.

Move to Preset: Causes camera to use its PTZ functionality to move to a specified preset upon alarm.

Notify Client: Sends a message to any clients currently connected to this camera when an alarm is triggered.

Record: Causes the alarm condition to result in recordings captured for the channels specified in alarms > Alarms Record Duration. The default value is the same camera number for which you have configured the current settings.

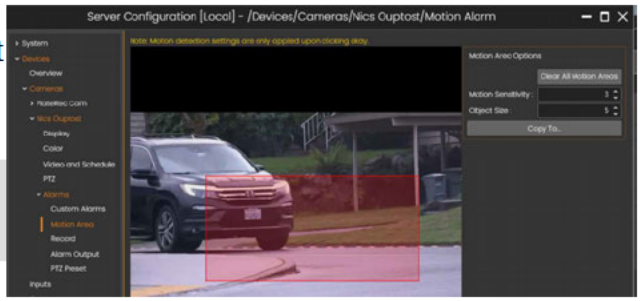
Send Email: Enables the sending of an email when an alarm is triggered.

Output to Relay: Causes alarm to output to previously set up Relay(s).

Motion Area

When the user uses motion detection, motion can be detected on the entire channel screen, or the user can select a subset of up to 7 manually configured motion detection areas.

📖 **IMPORTANT:** Not all IP cameras support the settings of motion areas; work with your integrator to accurately define your motion areas.



The default motion detection area covers the entire screen, so if any area is left undefined, the entire screen is used to detect motion.

Add New Motion Area: Click anywhere on the screen and drag to draw a rectangle of the area you want to select.

Clear All Motion Areas: Deletes all the previously created motion detection areas for this camera.

Motion Sensitivity: Controls the sensitivity of the motion alarm trigger. The lower the value, the higher the sensitivity.

Object Size: Sets the motion detection object size for this channel. 1 triggers for the smallest objects, 10 triggers for only the largest.

Motion Detection FPS: Sets the frames per second used in motion detection for this channel. Higher frame rates result in more accurate motion detection at the cost of CPU usage.

Record

When an alarm gets triggered for the selected camera and the recording option is checked in the General Settings tab, select the cameras that you want to be recorded. All cameras use the same 'Post Alarm Record' duration, but they use their individual recording quality settings as defined in the camera's settings.

Alarm Output

Select which Alarm Control to trigger as a result of any alarm on the current camera. Check the box of each relay you want to be triggered when a camera alarm occurs.

PTZ Presets

When an alarm gets triggered on the selected camera, the PTZ control can move the camera to the desired **preset** location. Double-click on the camera you want to move to a preset due to an alarm trigger.

Normal Preset: This is the PTZ preset to return to after that alarm duration ends.

Alarm Preset: This is the PTZ preset to move to when an alarm gets triggered.

©2021 Airship Industries

NEXUS VERSION HISTORY

7.2.0

- UI Redesign
- Added ability to search for options in settings window
- Added ability to show transcode profile information in OSD from Nexus VMS cameras
- Added support for discrete interpolation in Digital Zoom
- Improved UI for exporting map
- When using PTZ speed slider, tooltip will now show numerical value to indicate speed

[end]
rev:202112021640

©2021 Airship Industries


MASSACHUSETTS
STATE
POLICE

neology™
mobility [re]imagined™

497 Series ALPR Camera - Product Overview

Product Information pack

PRESENTER'S NAME

DATE

497 Series ALPR Camera Overview

Overview

Fully integrated ANPR camera with on board OCR



Performance

Optimised for Urban deployment
Two lane coverage (EU/UK)
0lux ANPR to 35m
High Resolution (1920x720) daylight and IR



Features

Fast Single cable installation
Secure data management
Integrated Neology OCR
AI analytics compatible

Copyright © 2021 Neology, All Rights Reserved.
Preliminary

subject to change without notice

497 product overview

- Fully integrated ANPR camera, with onboard OCR
- Designed for urban environments
- 0 lux ANPR operation to +35m
- Enhanced daylight overview camera*
- Reduced size (compared to IRIS)
- Fast, single cable installation
- Enhanced data security*

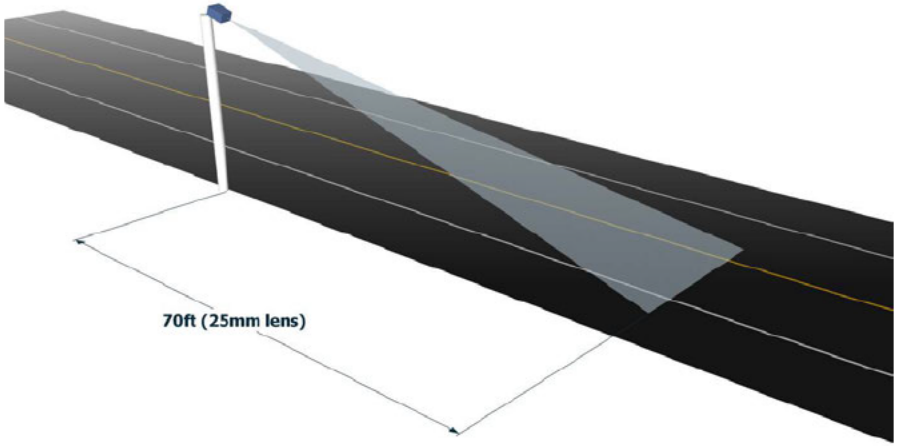


* Compared to previous generation P492

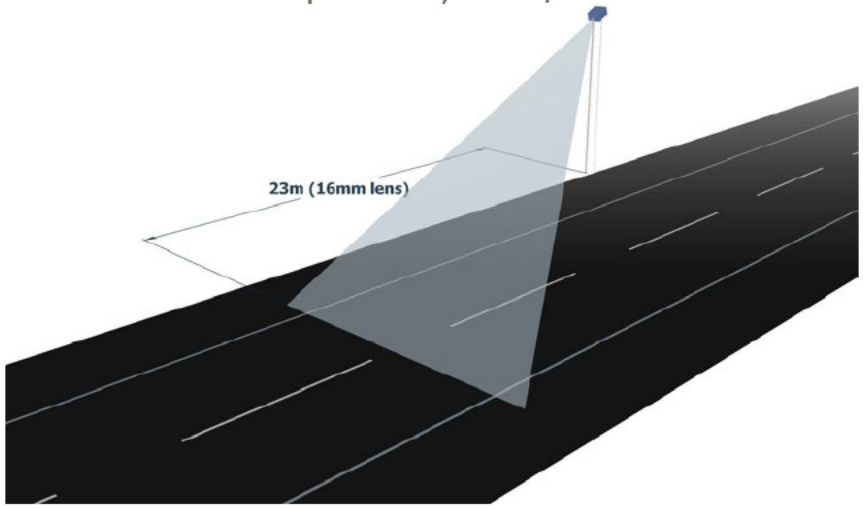
Copyright © 2021 Neology, All Rights Reserved.

Lane Coverage

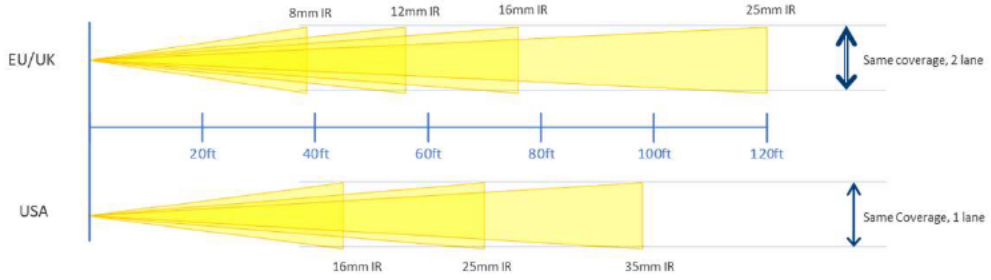
- Single lane operation, in US



- Dual lane operation, in UK/EU



Based on example of 120pix/plate, and a coverage of US = 16ft (4.8 m), Uk = 8.3m (27.3ft),



Copyright © 2021 Neology, All Rights Reserved.

Imaging capability

Overview

Clear high resolution overview images for vehicle color and model classification



IR ALPR

Clear images of both front and rear license plates ensures a high accuracy plate read is achieved regardless of vehicle direction



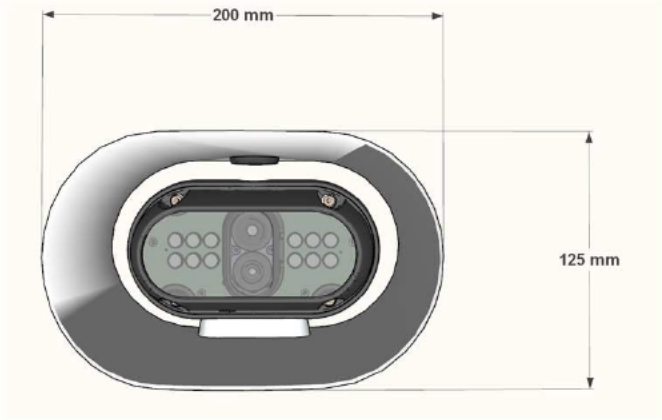
Copyright © 2021 Neology, All Rights Reserved.

Preliminary

subject to change without notice

Compact Design

- Reduced visibility in urban environments
- Optional hood colours (Black/white)
- Minimal footprint with ‘No hood’ operation for covert operations





497 (on left) compared to IRIS camera

Copyright © 2021 Neology, All Rights Reserved.

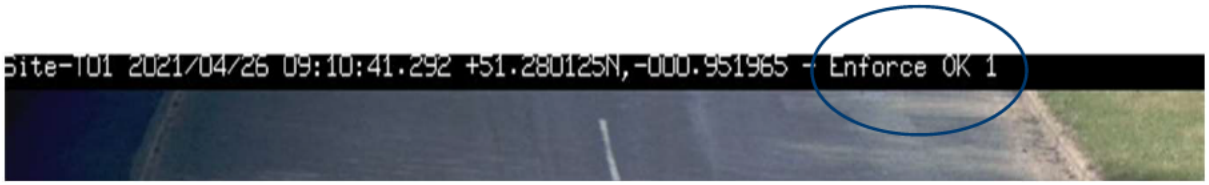
Enhanced Data Confidence

Disk encryption; data at rest on the camera is fully encrypted

Signed images; Image records can be individually signed to indicate authenticity

Enforcement mode; Image banner and Diagnostics reporting of camera status

Inbuilt firewalls, VPN and secure sockets support for communications



Copyright © 2021 Neology, All Rights Reserved.
Preliminary

subject to change without notice

Fast and Easy Install



Ethernet Connectivity



Single Cable, cable gland or connector options



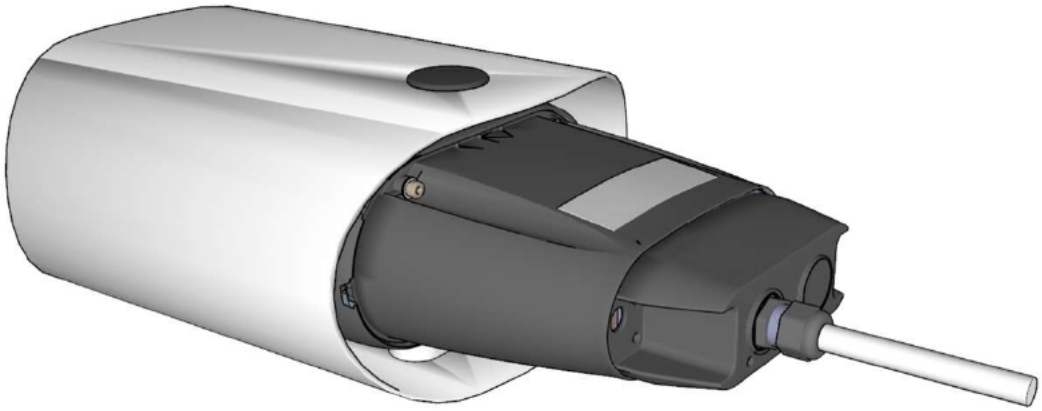
Accessories; Cables, Termination Boxes, Brackets and modem options



Rapid deployment with pre configured lenses and config management tools

Copyright © 2021 Neology, All Rights Reserved.

Camera cable termination



Cable Gland

- Cable passed through gland and secured with 'screw down' connector
- IP68 cable gland provides environmental protection and screen grounding

Copyright © 2021 Neology, All Rights Reserved.

Benefits and new features compared to 492

- Improved features over previous generation 492
  - More throughput, dual lane UK/EU
  - Security updates – data confidence!
  - Higher quality images and improved low light performance
  - Commonality to IRIS configuration management and tools
  - Latest CARDET updates
  - Deep learning AI services compatible
  - Easy retro fit to previous PiPS camera installations
  - Fast install – fixed lens, single cable, remote updates (OS, app, config)
  - Greater max working distance of over 30m

Copyright © 2021 Neology, All Rights Reserved.

End of Section

Copyright © 2021 Neology, All Rights Reserved.

neology™
mobility [re]imagined™

497 Series ALPR Camera – Optional Accessories

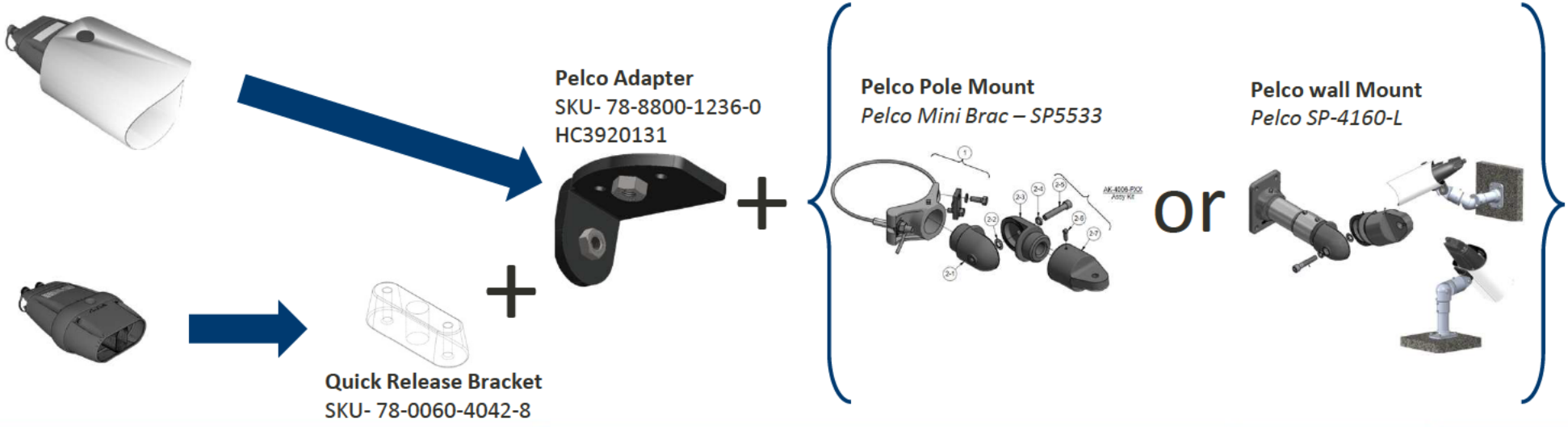
Preliminary Information pack - Subject to change without notice

PRESENTER'S NAME

DATE

Available accessories – Brackets, all territories

- Based on Pelco range of brackets for universal operation
- Option for mounting without hood for covert installs
- Add in urban mount bracket --TBC



Copyright © 2021 Neology, All Rights Reserved.
Preliminary

subject to change without notice

Available accessories – Brackets, all territories

- Based on Pelco range of brackets for universal operation
- Option for mounting without hood for covert installs
- Add in urban mount bracket --TBC

497 Series camera ***with*** hood





497 Series camera ***without*** hood

Hoodless mount bracket
SKU- HC3920120
(also known as the quick release bracket)

497 Series Pole Mount kit
SKU - FA349-0100-000



Contains:

Pelco Adapter
SKU- 78-8800-1236-0
HC3920131

Pelco Pole Mount
Pelco Mini Brac – SP5533
SKU 75-0302-2715-3

or

497 Series Wall Mount kit
SKU - FA349-01200-000



Contains:

Pelco Adapter
SKU- 78-8800-1236-0
HC3920131

Pelco wall Mount
Pelco SP-4160-L
SKU - TBC

Copyright © 2021 Neology, All Rights Reserved.
Preliminary

subject to change without notice

Available accessories – Brackets Pt1, all territories

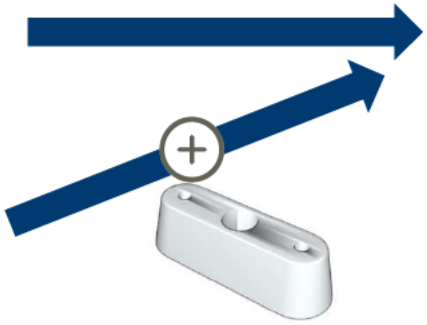
- Based on Pelco range of brackets for universal operation
- Option for mounting without hood for covert installs

497 Series camera ***with*** hood



497 Series camera ***without*** hood*





Hoodless mount bracket
SKU- HC3920120
(also known as the quick release bracket)

* Only for use in protected environments

497 Series Pole Mount kit
SKU - FA349-0100-000



Contains:

Pelco Adapter
SKU- 78-8800-1236-0
HC3920131

Pelco Pole Mount
Pelco Mini Brac – SP5533
SKU 75-0302-2715-3

or

497 Series Wall Mount kit
SKU - FA349-0200-000



Contains:

Pelco Adapter
SKU- 78-8800-1236-0
HC3920131

Pelco wall Mount
Pelco SP-4160-L
SKU -

Copyright © 2021 Neology, All Rights Reserved.

Available accessories – Brackets Pt2, all territories

- Based on Pelco range of brackets for universal operation
- Option for mounting without hood for covert installs

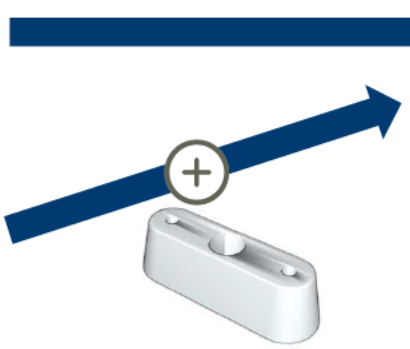
497 Series camera ***with*** hood



497 Series camera ***without*** hood*

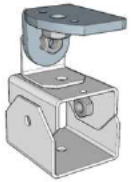


* Only for use in protected environments



Hoodless mount bracket
SKU- HC3920120
(also known as the quick release bracket)

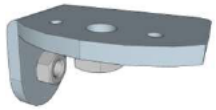
497 Series Urban Mount kit
SKU – HC3928401A



Contains:
- **Pelco Adapter**
  SKU HC3920131
- **Bracket L**
  SKU – HC3928411
- **Urban Bracket set**

or

497 Series Pelco Adapter
SKU – HC3920131



Contains:
- **Pelco Adapter only**
  SKU HC3920131

Copyright © 2021 Neology, All Rights Reserved.

Available accessories – T-Box and cables (USA)

- 1 or 2 camera options, based on IRIS version
- Now order cable separately – length option to suit camera



Cable unterminated
SKU- See 'Cable sheet for options and SKU's'

+

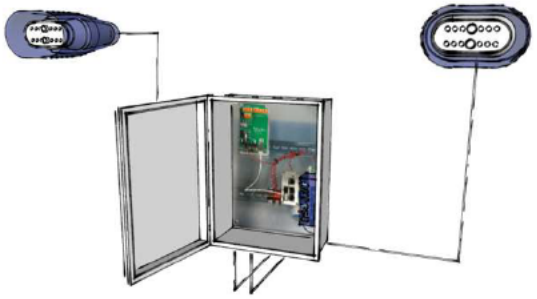
Single camera T-box
SKU- FA441-1100-000



Includes mounting brackets
Picture illustrative only

or

Dual camera T-box
SKU- FA441-2110-000



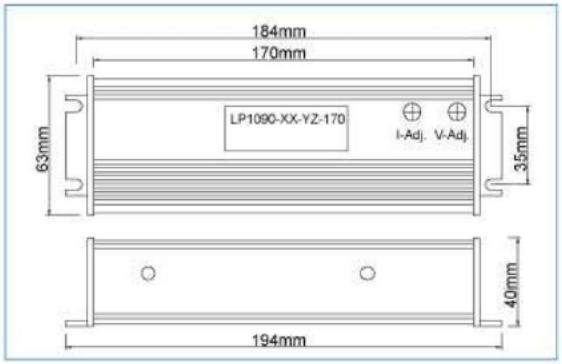
Includes mounting brackets
Picture illustrative only

Copyright © 2021 Neology, All Rights Reserved.

Available accessories – PSU (UK)

- IP66
- Suitable for lighting column mount
- SKU: 75030226726 PSU 19VDC/96W
  - Supplier Code (custom): Model LP-1090-19-GG-170-(18)-2M
  - 18V PSU, 2m input flying lead





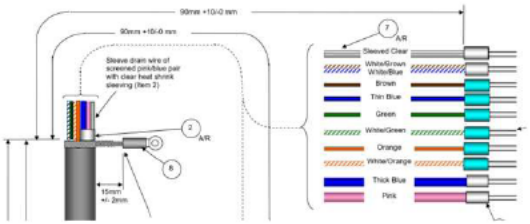
Copyright © 2021 Neology, All Rights Reserved.
Preliminary

subject to change without notice

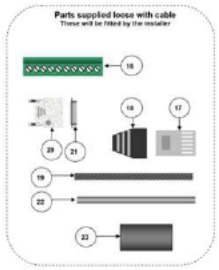
Available accessories – cables

- Single cable, Power and data (Not PoE)
- Neology Universal cable
- Various cable lengths (1,5,15,25,50,75m)

Cable XX meters, Glanded option
PIPS code- HC350228LXXX



Supplied with camera end fitted with ferrules,
Other end unterminated.
fitting accessories included



Note: RS232 terminator kit is not required

Copyright © 2021 Neology, All Rights Reserved.

Available accessories – External Modem, all territories

- Off the shelf third party item
- Global regional options
- IP67 LTE modem with Wifi
- PoE or DC supply
- Flexible connection options



Outdoor 4G LTE 150Mbps Router with dual sim slot (US)	FA501-4152-001
Outdoor 4G LTE 150Mbps Router with dual sim slot (UK)	FA501-4152-002

Manufacturer specifications available at the following web links:

https://www.outdoorrouter.com/product-category/outdoor-4g-lte-router/uk-4g-outdoor-router/
https://ezr33.outdoorrouter.xyz

Copyright © 2021 Neology, All Rights Reserved.

End of Section

Copyright © 2021 Neology, All Rights Reserved.

neology™
mobility [re]imagined™

Click to add text

497 Series ALPR Camera – Operational Scenarios

Preliminary Information pack - Subject to change without notice

PRESENTER'S NAME

DATE

Operational scenarios – configuration options - WIP

- New install
- 492 site upgrade
- Tbox, non-tbox US..????
- Column UK

Copyright © 2021 Neology, All Rights Reserved.

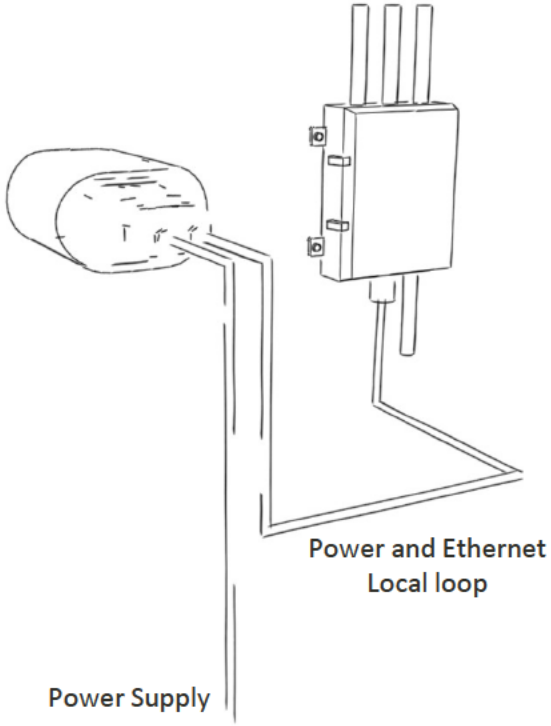
Upgrade a P492 site to use a 497

- Similarities
  - The physical envelope and mounting arrangement of the 492 and 497 are identical. (an additional adapter block is available is using a 'hoodless' installation)
  - There are however two body types, providing a glanded or connectorized cable connection. This is a factory fit option, and so must be specified at the point of order
  - The 497 can use the existing P492 PiPS universal cable, providing it is in good condition and fit for purpose. Note this only applies to the glanded version of the 497.

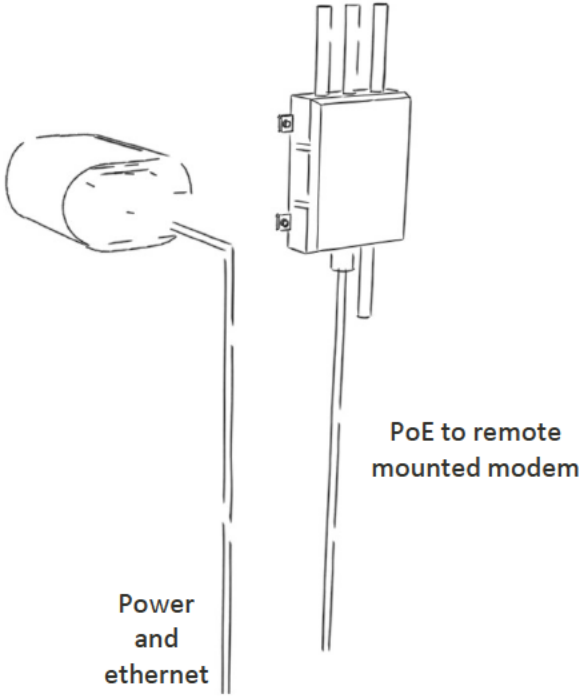
- Important Differences
  - The power supplies are different – the 497 is 12-24v, and is notionally 15Vmax for a Tbox installation. A 18V PSU is available for other installation types
  - A range of lens options is available, as per the P492, but the working distances are different due to the change in sensor geometry. An existing installation may need realignment.
  - There is no internal GPS or modem option.
  - The application SW is based on IRIS baseline, and so any configuration/interaction/management of the previous camera will need to be reviewed and updated.

Copyright © 2021 Neology, All Rights Reserved.

Modem Connection concept examples - draft



Local external Modem
- Power pass through from camera
- Ethernet and power from camera to locally mounted modem



Remote external Modem
- Power and ethernet connection to camera
- PoE Ethernet connected to modem via service point

Copyright © 2021 Neology, All Rights Reserved.





PIPS TECHNOLOGY™

DETECTION INNOVATION

Automated License Plate Recognition System

Cameras Using the Camera Interface Box

Installation Guide

NEOLOGY™ MOBILITY TECHNOLOGIES

© PIPS™ 2016. All rights reserved. PIPS™ is a trademark of Neology™.

The PIPS™ products described in this book are licensed products of PIPS™ Company or its affiliates. PIPS™ is a trademark of Neology™. Google Chrome is a trademark of Google Inc. Mozilla Firefox is a registered trademark of the Mozilla Foundation. Cradlepoint® is a registered trademark of Cradlepoint, Inc. All other trademarks and tradenames are property of their respective owners.

The PIPS™ products described in this book are licensed products of PIPS™ or its affiliates.
Information in this document is subject to change without notice. It is the responsibility of the user to comply with all applicable laws including confidentiality, privacy and copyright laws.

PIPS™ may have additional patents, patent applications, trademarks, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from PIPS™ Company, the furnishing of this document does not grant you any license to these patents, trademarks, copyrights, or other intellectual property.

No further publication or commercial use may be made of these materials without the express written permission of PIPS™.

Contents

Chapter 1. Safety Information 6
Intended Use 6
Chapter 2. Regulatory Information 8
RoHS Status 8
WEEE Compliant 8
FCC Class A Digital Device: 8
Canada Class A Compliance: 8
Europe Emissions Compliance: 8
Chapter 3. Intro to the PIPS™ ALPR System 9
ALPR or ANPR? 9
Introducing the PIPS™ High Resolution ALPR Camera 10
Introducing the PIPS™ Fixed ALPR Camera 10
Introducing the Fixed Wide Lane ALPR Camera 10
Chapter 4. Specifications 11
Model P382 Specifications 11
Model P392+ Specifications 11
Model P492 Specifications 11
Camera Interface Box Specifications 12
Performance Specifications 12
Chapter 5. Site Requirements 13
General requirements 13
Camera Deployment 13
Model P382 13
Model P392+ 13
Model P492 14
Networking Requirements 14
Chapter 6. Installation 15
Step 1: Install the PIPS™ Camera Toolkit 15
Step 2: Install the Camera Interface Box 15
Mounting Options 15
Mounting the Camera Interface Box to a Utility Pole 16
Mounting the Camera Interface Box to a Wall 17
Step 3: Mount Brackets and Cameras 18
General Mounting Instructions 18
About Mounting Brackets 18
About the Universal Bracket (75-0302-2230-3) 19
Camera Mounting Options with the Universal Bracket 20
Mounting the Universal Bracket and the Camera to a Horizontal Pole 21
Mounting the Universal Bracket and the Camera to a Vertical Pole 22
Mounting the Universal Bracket and the Camera to a Wall 23
Step 4: Make Camera-Side Cable Connections 24
Cabling the P382 Camera 24

Cabling the P392+/P492 Camera 25
Connect the Universal Cable to the Interface Module 29
Introduction 29
Step 5: Connect the Camera Interface Box to the Main 35
Step 6: Power on the Camera Interface Box 36
Step 7: Configure Network Settings on Your Laptop 36
Step 8: Set up a Connection to the Customer's Network 37
Connecting Using Ethernet 37
Connecting Using the Cradlepoint Modem 38
Step 9: Set up Cameras with the Toolkit 39
Step A: Connect to the Cameras 39
Step B: Change the Camera TCP/IP Settings 39
Step C: Invert the P392+/P492 Video 40
Step D: Align Cameras 41
Chapter 7. Camera Maintenance 43
Appendix A. Cabling Reference 44
Appendix B. RS-232 Default Settings 45
Appendix C. Firewall Settings 46
Appendix D. Product Warranty 47
PRODUCT USE STATEMENT 47

Chapter 1.
Safety Information

Please read, understand, and follow all safety information contained in these instructions prior to the use of this camera system. Retain these instructions for future reference.

Intended Use

This camera system is intended to provide monitoring and identification of vehicles in an outdoor environment. This camera system is used for industrial monitoring such as law enforcement, campus security, and tolling applications. It is expected that all users be fully trained in the safe operation of this camera system. Use in any other application has not been evaluated by PIPS™ and may lead to an unsafe condition.

Explanation of Signal Word Consequences	
⚠ **WARNING**	Indicates a hazardous situation, which, if not avoided, could result in serious injury or death.
⚠ **CAUTION**	Indicates a potentially hazardous situation, which, if not avoided, could result in minor or moderate injury and/or property damage.
⚠ **NOTICE**	Indicates a situation, which, if not avoided, could result in property damage.

Explanation of Safety and Related Symbols	
⚠ **WARNING**	Hazardous Voltage.
⚠ **CAUTION**	Lifting hazard.

WARNING

- **To reduce the risks associated with hazardous voltage, fire, and impact:**
  - Only follow installation procedures in the Installation Guide.
  - Only qualified personnel should install, maintain, or service the system.
  - Installation and service activities must be in compliance with all local, regional, and national applicable building and electrical codes.
- **To reduce the risks associated with hazardous voltage and fire:**
  - Disconnect AC power from the termination box when connecting or disconnecting components of the system.
  -Ensure that power cannot be restored inadvertently.
- **To reduce the risks associated with hazardous voltage:**
  -Use only with PIPS-approved power supplies listed in manual.
  -System is not rated for safe use with any power supply not specified by PIPS.
- **To reduce the risks associated with fire:**
  -Leave sufficient space around all electrical components for cooling.
  -Do not mount any electrical components directly above a heat source.
- **To reduce the risk associated with impact:**
  -Install only using PIPS™ supplied mounting brackets.
  -Ensure that all hardware is firmly tightened before loading.
  -Installation and service activities must be in compliance with all applicable building and electrical codes.
  -Any mounting surface must be able to support a minimum static load of equal to the maximum weight of the fixed camera system plus any additional live load due to environmental conditions.

CAUTION

- **To reduce the risks associated with impact, muscle strain:**
  - Use appropriate PPE and follow safe workplace practices during installation.
- **To reduce the risks associated with muscle strain:**
  - Use appropriate mechanical or human assistance when lifting system components.
- **To reduce the risks associated with environmental contamination:**
  - Dispose of all system components in accordance with applicable local and government regulations.

NOTICE

- **To reduce the risk of property damage:**
  - Do not modify or attempt to service the camera. Return to PIPS authorized service centers for repair or service. There are no user serviceable parts.
  - Do not use solvents or harsh cleaners on camera.
  - Do not use abrasive materials on camera window.

Chapter 2.
Regulatory Information

This product complies with the following standards:

- UL 60950-1
- CSA 60950-1
- EN 60950-22
- EN 60950-1
- IEC 60950-1

This device is “listed” and carries the cULus listing mark based on compliance to the above UL standard.

The PIPS™ camera system is CE marked for conformity to current European R&TTE, Low Voltage, and EMC directives. Declaration of Conformity is available upon request.

RoHS Status

The PIPS™ Fixed ALPR Systems for Law Enforcement or Campus Security fall within Category 9 of the EU’s RoHS Directive 2011/65/EU, referred to as RoHS 2, “Monitoring and Control Instruments, including Industrial Monitoring and Control Instruments” with a required compliance date of July 22, 2017. A Declaration of Conformity is available upon request.

WEEE Compliant

At the end of its useful life, this product pursuant to European Directive 2003/108/CE and its implementation in national law, must not be released into the environment or thrown away as domestic waste, but must be disposed of at an authorized recycling center (contact the relevant local authorities for a list of places where the product may be disposed of according to the law). Disposing of the product correctly contributes to protecting human health and safeguarding the environment.



FCC Class A Digital Device:

This industrial equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her expense.

The product may include a wireless Cradlepoint broadband router with FCC ID:
UXX-IBR600E and IC ID: 6921A-IBR600E.

Modifications not expressly approved by PIPS™ could void the user’s authority to operate the equipment under FCC rules.

Canada Class A Compliance:

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la NMB-003 du Canada.

Europe Emissions Compliance:

This equipment is considered Group 1; Class A industrial equipment according to IEC/CISPR 11. Without appropriate precautions, there may be potential difficulties ensuring electromagnetic compatibility in other environments due to conducted as well as radiated disturbance.

Chapter 3.

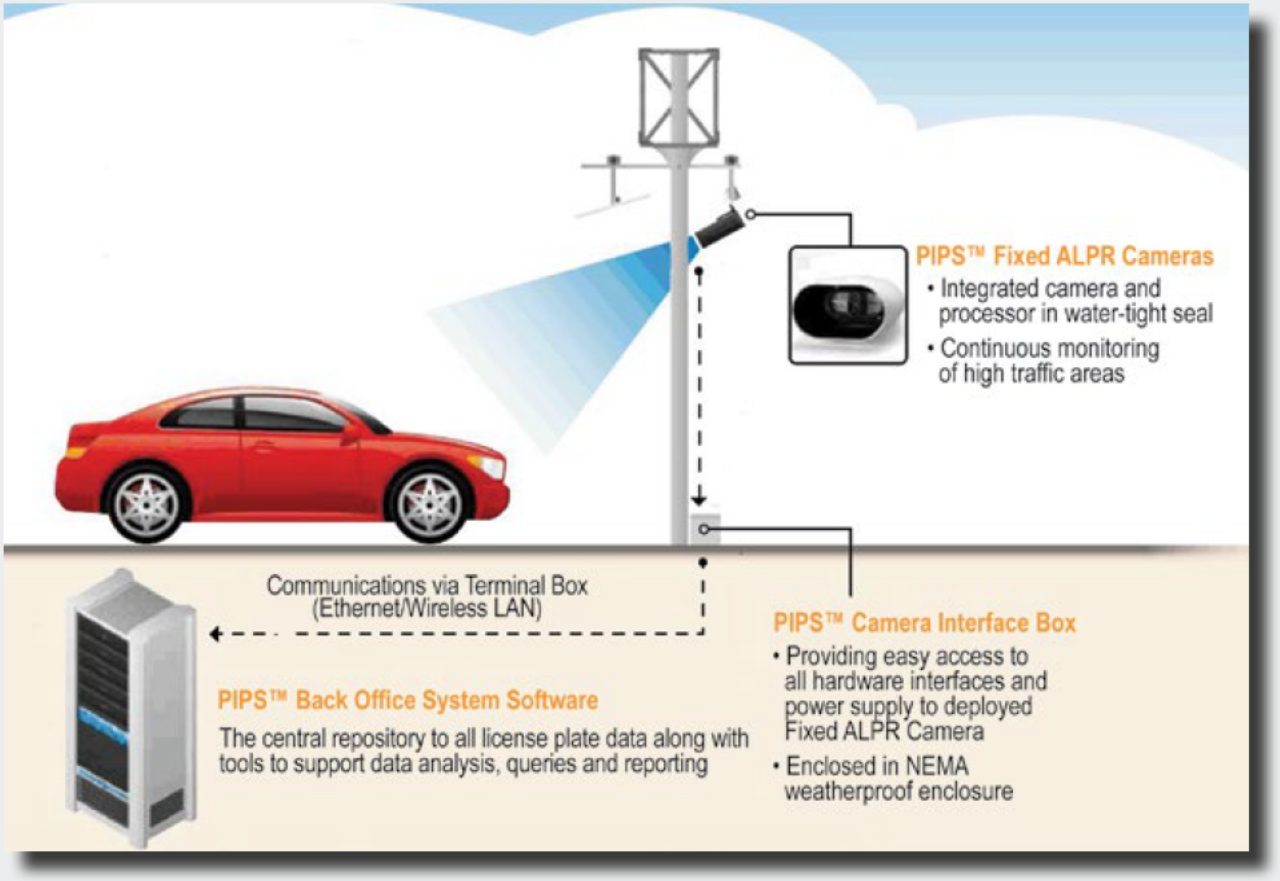
Intro to the PIPS™ ALPR System

This manual introduces the PIPS™ Automated License Plate Recognition (ALPR) system and explains how to install the Camera Interface Box and P382, P392+, and P492 cameras.

Information on back office software installation and configuration can be found n a separate software manual.

ALPR or ANPR?

This manual refers to the technology as Automated License Plate Recognition, or ALPR. This same technology is sometimes called Automated Number Plate Recognition, or ANPR, which is the name the software component of this system uses. The different names derive from what vehicle identification plates are called throughout the world, license plates or number plates. Keep in mind that these names refer to the same thing.



Introducing the PIPS™ High Resolution ALPR Camera

The PIPS™ High Resolution ALPR Camera Model P382 can provide up to 15.84 ft./4.83 m of horizontal traffic lane coverage while capturing multiple license plates in the same field of view. This fully integrated ALPR unit can be configured in minutes. Quality lenses used in the P382 provide customers with the sharpest IR image quality available within the PIPS fixed camera family. No moving parts in a water-tight housing provide added durability in a variety of operating conditions.



Introducing the PIPS™ Fixed ALPR Camera

The 3M™ Fixed ALPR Camera Model P392+ is a fully-integrated ALPR unit incorporating camera, illuminator, and image processing within a single water tight, sealed enclosure. This ALPR camera provides customers with 5.5 ft. of horizontal traffic lane coverage, and its smaller size (as compared to the rest of PIPS™ fixed camera family) makes it the perfect solution for single lane coverage in dense locations, such as busy intersections.



Introducing the Fixed Wide Lane ALPR Camera

Our newest member of the PIPS™ fixed camera family, the PIPS™ Fixed Wide Lane ALPR Camera Model P492, sets itself apart with its unique performance capabilities. This fully-integrated ALPR unit captures multiple license plates in the same field of view across 23.3 ft. / 7.1 m of traffic lanes. It is designed to utilize smaller, high power LEDs and provides the best color overview image resolution offered by PIPS™ ALPR cameras.



Chapter 4.
Specifications

Model P382 Specifications

Dimensions (L x W x H)	16.9 x 10.3 x 9.1 in. / 430 x 260 x 230 mm (including hood) 8.5 x 9.2 x 5.8 in. / 215 x 234 x 148 mm (excluding hood)
Weight	17 lbs. / 7.7 kg (including hood) 16.5 lbs. / 7.5 kg (excluding hood)
Power	36 to 55 VDC (48 VDC Nominal)
Operating Temperature	-40° to +140 °F / -40° to +60° C

Model P392+ Specifications

Dimensions (L x W x H)	Including hood Excluding hood	14.2 x 8.7 x 5.2 in. / 361 x 221 x 132 mm 8.7 x 6.6 x 3.6 in. / 221 x 168 x 91 mm OR 9.8 x 6.6 x 3.6 in. / 249 x 168 x 91 mm (Length difference depends on lens focal length)
Weight	Including hood Excluding hood	5.18 lbs./2.35 kg 3.31 lbs./1.5 kg
Power	N/A	12 to 24 VDC (18 VDC nominal)
Operating temperature	N/A	5° to +140° F / -15° to +60° C

*IEC/EN 60950-22 compliant to 5° F /-15° C. 3M verified to continuously read license plates at - 40° F / -40 C°.

Model P492 Specifications

Dimensions (L x W x H)	Including hood Excluding hood	15.7 x 7.9 x 4.7 in / 399 x 200 x 119 mm 8.7 x 6.5 x 3.6 in / 220 x 166 x 91 mm Or 9.8 x 6.5 x 3.6 in / 249 x 166 x 91 mm (Length difference depends on lens focal length)
Weight	Including hood Excluding hood	5.6 lbs. / 2.55 kg 3.6 lbs. / 1.65 kg
Power	N/A	35 to 60 VDC (48 VDC Nominal)
Operating temperature	N/A	-40° to +140° F / -40° to +60° C

Camera Interface Box Specifications

Dimensions (L x W x H)	18.5 x 14.5 x 7.5 in / 470 x 368 x 191 mm
Weight	34 lbs / 15,4 Kg
Operating Temperature	-40° to 140° F / -40° to 60° C
Relative Humidity	90% (non-condensing)
Maximum altitude	6561 ft./2000 m
Voltage Range	100-240 VAC
Frequency	50-60Hz
Current	5 Amps / 225 W Max
Installation/Over Voltage	Category II Pollution Degree 3
Duty Cycle	Continuous

Performance Specifications

Attribute	Model P382	Model P392+	Model 492
PIPS™ name	PIPS™ High Resolution ALPR Camera	PIPS™ Fixed ALPR Camera	PIPS™ Fixed Wide Lane ALPR Camera
IR Resolution	1392 x 512	752 x 480	2048 x 720
Overview Resolution	720 x 288	752 x 480	2048 x 720
Lens Type	C-Mount	S-Mount	S-Mount
Frame Rate Frequency	50 fields per second	50 fields per second	50 fields per second
CPU	500 MHz	1.2 GHz	1.2 GHz
RAM	256 M	256 or 512 M	512 M
LEDS	264	96	44
Invertible	N	Y	Y
Color Overview	Y	Y	Y
Road Width Coverage EU	15.84 ft./4.83 m	8.56 ft./2.61 m	23.3 ft./7.1 m
Road Width Coverage U.S.	9.14 ft./2.79 m	4.94 ft./1.51 m	13.44 ft./4.1 m
Max Focus Distance UK	132.2 ft./40.3 m	94.49 ft./28.8 m	103.3 ft./31.5 m
Max Focus Distance US	77.4 ft./23.6 m	55.5 ft. /16.9 m	60.7 ft./18.5 m
Connector type	Gland	Gland	Gland

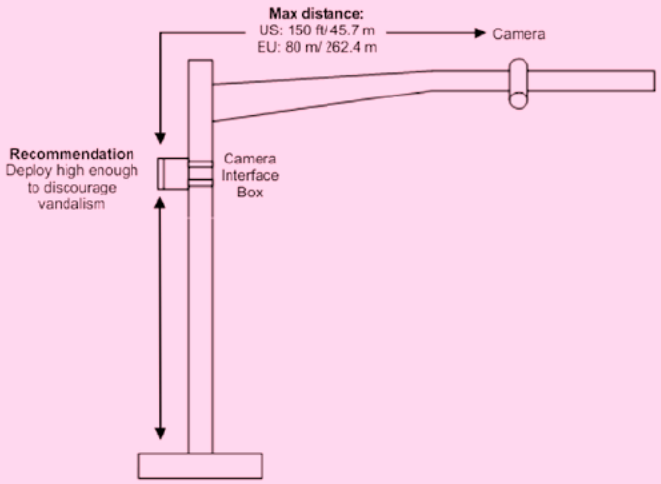
Chapter 5.

Site Requirements

General Requirements

The site where the camera interface box and cameras are deployed must comply with requirements listed in Specifications on page 11.

- The camera interface box and cameras must be no further apart than 80 meters / 262.4 ft.
- The camera interface box and cameras should be deployed high enough off the ground to discourage vandalism and to prevent contact by passers-by.
- If Ethernet will be used to communicate with the back office server, the maximum distance between the camera interface box and the server itself or an Ethernet router, switch or hub is 328 ft. / 100 m.



Camera Deployment

The lens with which the camera was fitted will determine the optimum distance between the camera and the license plates it will read. This section provides information on the recommended distance between the two.

Model P382

Lens Focal Length (mm)	Focal distance U.S. Plates	Focal distance U.S. Plates
75	40.3 m	80 ft.
50	26.9 m	54 ft.
35	18.8 m	36 ft.
25	13.4 m	28 ft.

Model P382

Lens Focal Length (mm)	Focal distance U.S. Plates	Focal distance U.S. Plates
50	31.5 m	60.6 ft.
35	22.1 m	42.5 ft.
25	15.8 m	30.3 ft.

Model P392+

Lens Focal Length (mm)	Focal distance U.S. Plates	Focal distance U.S. Plates
50	40.3 m	80 ft.
35	26.9 m	54 ft.
25	18.8 m	36 ft.
18.5	13.4 m	28 ft.
18.5	13.4 m	13.4 m
18.5	13.4 m	13.4 m

Networking Requirements

Cameras can communicate with back office software using either a wired Ethernet connection or a cellular modem connection. Technicians setting up these connections will require the following:

A static IP address for each camera

- The following for the modem connection, if it is used:
  - An APN (access point name), which is the name of the gateway the modem will use for communication over the Internet
  - No incoming/outgoing ports blocked on the network

Chapter 6.
Installation

Follow steps in this section to install the camera and power supply unit.

Step 1: Install the PIPS™ Camera Toolkit

You will need the PIPS™ Camera Toolkit on your laptop to complete installation.
Note: The toolkit requires Windows 7.

How to Obtain the PIPS™ Toolkit Software
To obtain the software, contact your local support team:
- Europe, Middle East and Africa: support@pipstechnology.co.uk
- U.S.: support@pipstechnology.com

To install the program
- Download the file to your laptop, double click the executable, and respond to the installation prompts.

Notes:
- The "PIPS™ Streamer" application is not required; it is for older cameras.
- Previous versions of the Toolkit installed and used ActivePerl. If a copy of ActivePerl is found during installation, the installation program will offer to remove it. If you are sure that you do not use ActivePerl for anything else, click "Yes."
- The Toolkit package includes a program for reading .axi files created by cameras. If you want the axireader.exe to be run whenever .axi files are selected, click "Yes" on the axireader dialogue box.

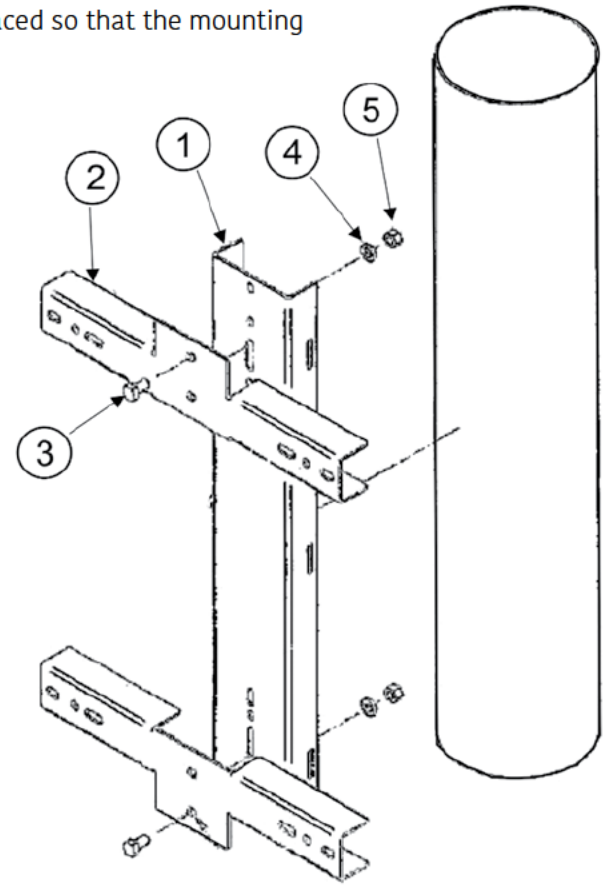
Step 2: Install the Camera Interface Box

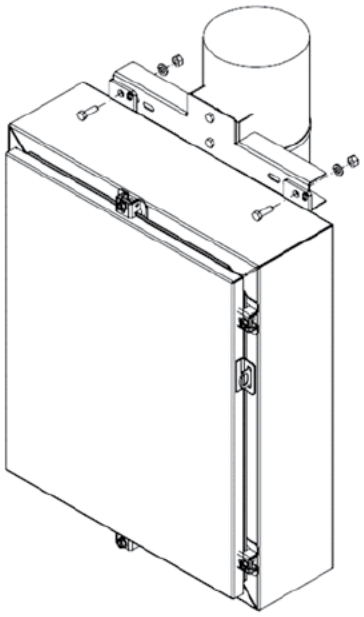
Mounting Options
You can mount the camera interface box on the following:
• A horizontal or vertical utility pole. (See Mounting the Camera Interface Box to a Utility Pole on page 16).
• A wall (See Mounting the Camera Interface Box to a Wall on page 17.

Mounting the Camera Interface Box to a Utility Pole
1. The pole mounting components can be purchased from Hammond Mfg, 1 EA of: PMV1216GY; PMH15GY; and PMSTRAP55, These components supply the following:

Item	Description	Qty.
1	Vertical Rail	60.6 ft.
2	Horizontal Rail	42.5 ft.
3	3/8" – 16 x 3/4" Bolt ZP	30.3 ft.
4	3/8" Split Lock Washer ZP	15.8 m
5	3/8" – 16 Hex Nut ZP	15.8 m
6	PMSTRAP (stainless steel strap)	15.8 m
7	5/16" – 18 x 1" Bolt ZP	15.8 m
8	5/16" Split Lock Washer ZP	15.8 m
9	5/16" – 18 Hex Nut ZP	15.8 m

2. Lay the two horizontal rails (#2) along the vertical rail (#1), spaced so that the mounting tabs on the interface box will line up with mounting holes.
3. Connect hardware as shown.





4. Insert bolts (#7), split lock washers (#8) and hex nuts (#9) to the outside holes of the top and bottom rails and tighten bolts and nuts.

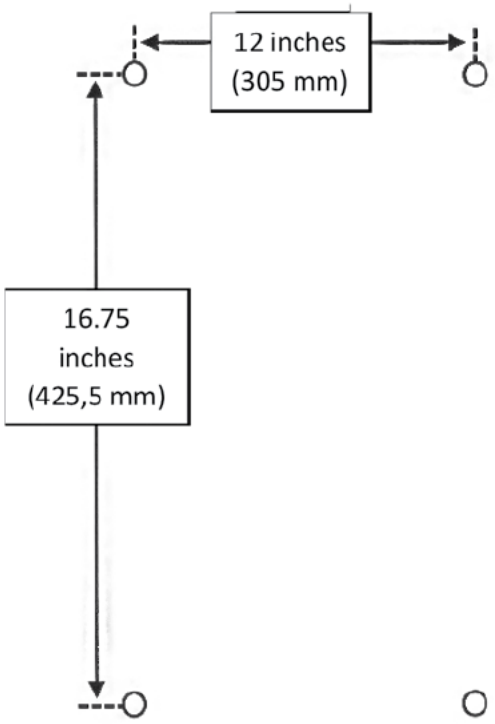
Mounting the Camera Interface Box to a Wall

Hardware Requirements

Walls with studs	• Flange Head Lag Screw for Wood (Quantity 4) • Hot-Dipped Galvanized Steel, 5/16 in / 8 mm diameter and 2 in /51 mm long
Walls of concrete, block, brick	• Stud Anchors for Concrete, Block and Brick 5/16 in / 8 mm diameter, thread 1/4 in-20 / 6.35 mm -20; • Washer OD: 11/16 in / 17.5 mm (Drill size 5/16 in / 8 mm

Mounting on Walls with Studs

Due to weight, the enclosure must be mounted to the wall frame (studs). If the studs are not aligned with the hole locations, create a rectangular frame (using wood 2x4) that fits the enclosure hole locations and existing studs. Use a level to ensure even distribution of weight.



Mounting on Concrete, Block, or Brick

1. Determine the hole locations on the wall (or frame).
2. Pre-drill the holes using 5/16 in / 8 mm drill size for concrete, block and brick wall.
3. Drill the bottom screws and leave about 3/8 in./9.5 mm gap to the wall.
4. Slide the bottom of the enclosure onto those screws and push the top end against the wall and drill the top two screws.

Step 3:Mount Brackets and Cameras

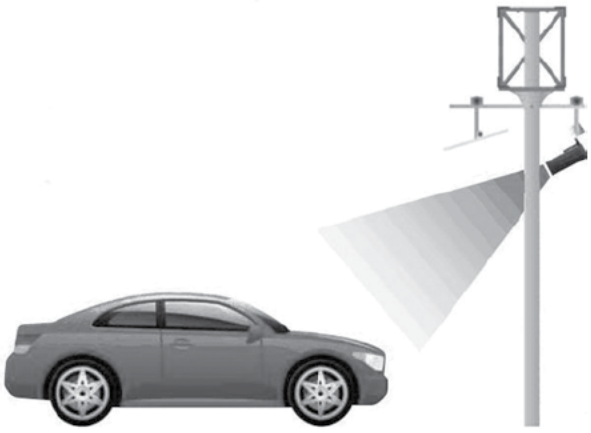
General Mounting Instructions

The camera should be mounted so that it has a clear view of the roadway at the correct focal distance.

The camera should be mounted at an angle no greater 30 degrees; OCR failure should be expected at angles greater than 45 degrees.

Vehicles must enter the top or bottom of the field of view and leave via the top or bottom. They must not traverse the field of view sideways.

Note: The P382 does not support the image flipping feature, so it must be mounted in the correct orientation, with the top of the camera on top.



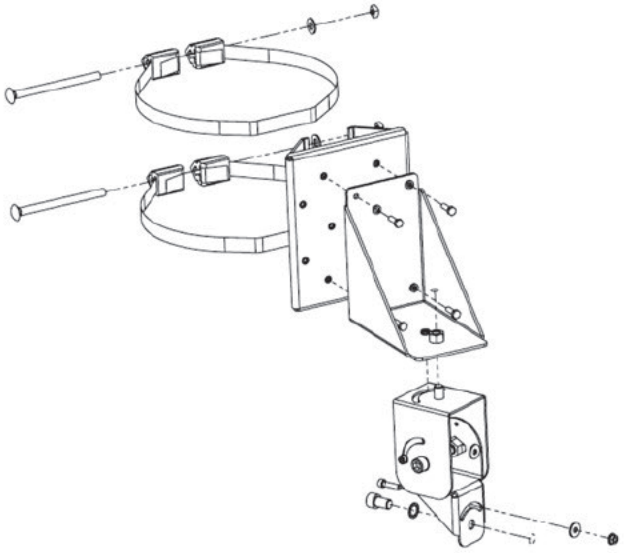
About Mounting Brackets

There are four supported mounting brackets. Locate the information that applies to the bracket you will be using:

- About the Universal Bracket (75-0302-2230-3) on page 19
- Camera Mounting Options with the Universal Bracket on page 20
- Mounting the Universal Bracket and the Camera to a Horizontal Pole on page 21
- Mounting the Universal Bracket and the Camera to a Vertical Pole on page 22
- Mounting the Universal Bracket and the Camera to a Wall on page 23

Camera Interface Box Specifications

The universal bracket is a set of modular components that allows for the installation of any PIPS™ ALPR camera to horizontal or vertical poles and flat surfaces. By combining various bracket elements, the installer should be able to position the camera so it has a proper field of view.



The universal bracket consists of the following:

- Urban bracket
- Pole mount plate
- Wall bracket
- Banding
- Banding clips

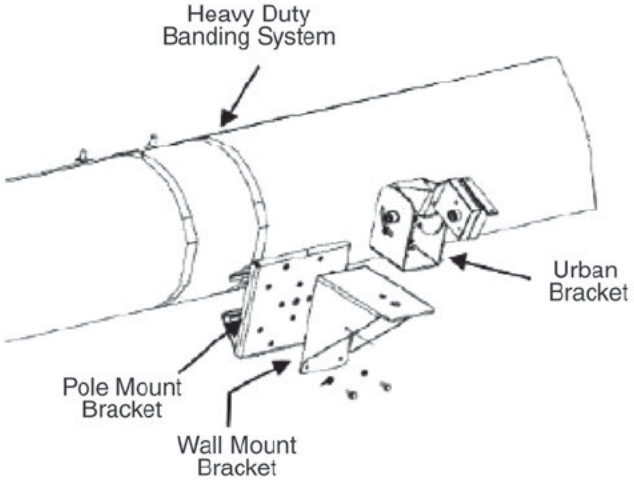
The urban bracket provides a mounting surface to attach any camera to one side or the other, to a wall bracket or a pole mount plate. The bracket provides a number of options that the installer can use to adjust the vertical tilt and horizontal angle of the camera to achieve the best field of view.
The pole mount plate provides a means to attach other components of the universal bracket to the metal bands that are used to hold the bracket assembly to a pole.

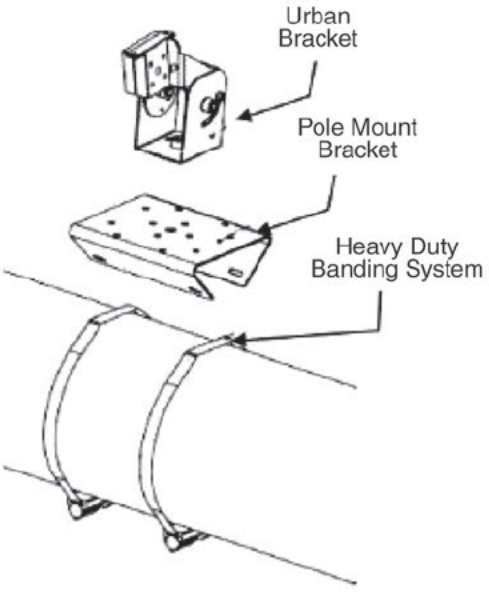
The pole mount plate has a variety of pre-tapped holes that allow the installer to attach either a wall mount bracket or urban bracket to it.

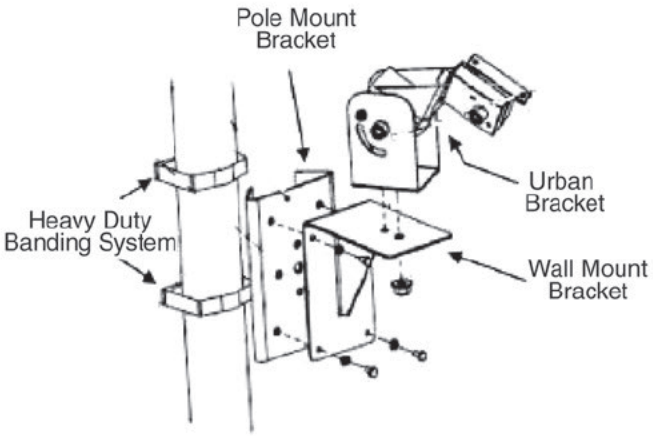
The wall bracket, a reinforced right angle bracket, can be attached to a flat surface or pole mount plate on one side and the urban bracket on the other. The other side of the bracket has a nut welded to it to allow for connection to the quick release on the urban bracket.

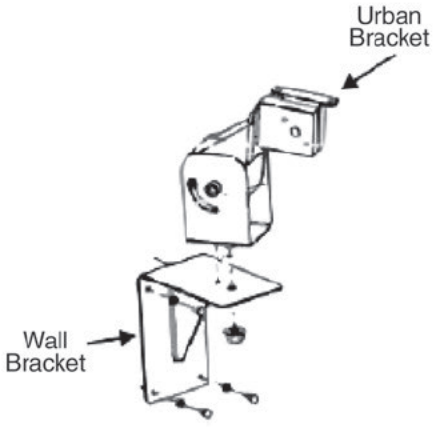
Banding and banding clips attach the universal bracket system to a circular pole. These standard components consist of two stainless steel bands 0.75 in./1.9 cm wide by 56 in./142.2 cm long; four banding clips and two securing bolts, washers and nuts. These standard length bands allow the installation of the bracket to a pole that is 8 in./20.3 cm to 14 in./35.6 cm in diameter. Poles greater than 14 in./35.6 cm in diameter require special order bands. Poles that are less than 8 in./20.3 cm in diameter require crimp banding.

Camera Mounting Options with the Universal Bracket









Mounting the Universal Bracket and the Camera to a Horizontal Pole

Follow these instructions to install camera brackets to a horizontal pole.

1. Locate the following for each camera:
   - Urban bracket
   - Pole mount plate
   - Wall bracket
   - Banding and banding clips

2. Ensure that you have the following tools with you:
   - Tape measure
   - Mallet
   - Metal cutters
   - Torque wrench
   - Marker
   - Allen wrenches

Notes:
- Assemble the urban bracket to the wall mount bracket on the ground if you are using both elements of the bracket system.
- Prepare banding on the ground, not in the bucket truck or lift.

3. Measure the circumference of the pole.

4. Add 12 in./30.5 cm to the circumference of both bands and then cut them.

5. Mark the bands 6 in./15.2 cm from each end.

6. Pull both bands through the pole mount plate.

7. Locate clips with chamfered cone drilled out. Make sure one clip with chamfered cone is on each band.

8. Place clips onto each band so that the bolts through the holes face outward and the bands bend back against the beveled edge of the clip.

9. Bend 6 in./15.2 cm of banding underneath the clips.

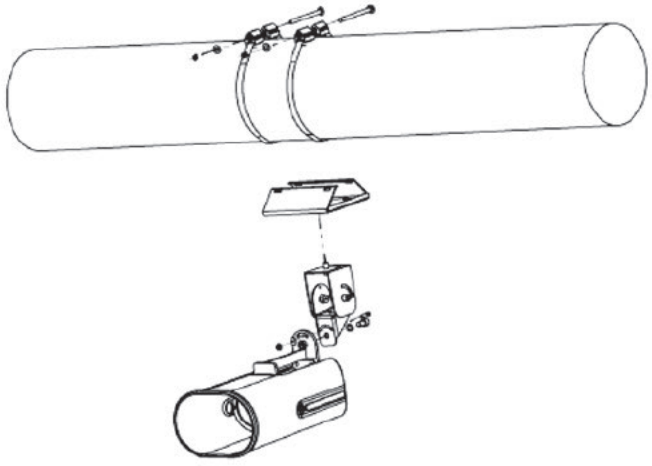


Figure 1 P382 beneath Horizontal Pole

10. Place the prepared pole bracket assembly on the pole and place bolts through the clips without chamfered cone.

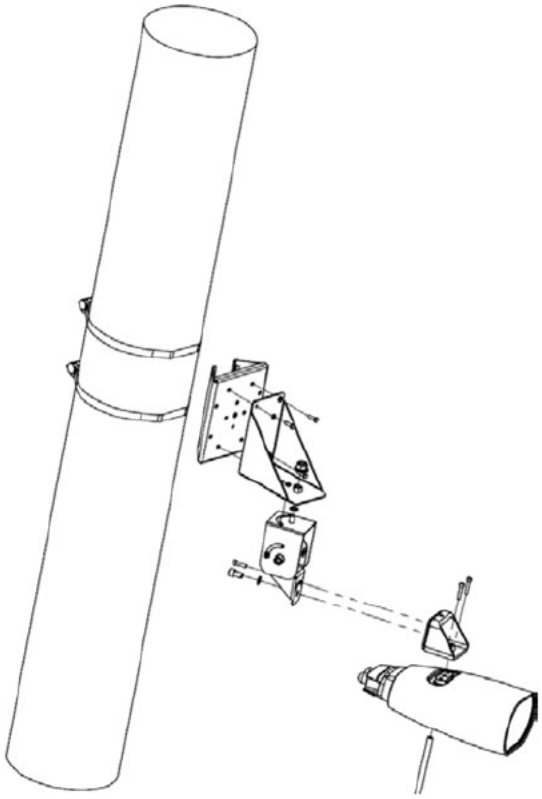
11. Torque bolts to 30 ft. lbs. / 41 newton meters.

12. Attach the remaining hardware (wall mount bracket and urban bracket). Add Nordlock washers under the bolt heads of the fasteners that fasten the urban bracket to the wall mount.

13. Mount the camera as shown in the illustrations. Do not tighten the mounting hardware fully until the alignment is complete.

Mounting the Universal Bracket and the Camera to a Vertical Pole

Follow these instructions to install camera brackets to a vertical pole.



1. Locate the following for each camera:
• Urban bracket
• Pole mount plate
• Wall bracket
• Banding and banding clips

2. Ensure that you have the following tools with you:
• Tape measure
• Mallet
• Metal cutters
• Torque wrench
• Marker
• Allen wrenches

Notes:
• Assemble the urban bracket to the wall mount bracket on the ground if you are using both elements of the bracket system.
• Prepare banding on the ground, not in bucket truck or lift.

3. Measure the circumference of the pole.

4. Add 12 in./30.5 cm to the circumference of both bands and then cut them.

5. Mark the bands 6 in./15.2 cm from each end.

6. Pull both bands through the pole mount plate.

7. Locate the clips with chamfered cone drilled out. Make sure one clip with chamfered cone is on each band.

8. Place the clips onto each band so that the bolt through the holes faces outward and the bands bend back against the beveled edge of the clips.

9. Bend 6 in./15.2 cm of the bands underneath the clips.



10. Place the prepared pole bracket assembly on the pole and place bolts through the clip without the chamfered cone.

11. Torque bolts to 30 ft. lbs. / 41 newton meters.

12. Attach the remaining hardware (wall mount bracket and urban bracket). Add Nordlock washers under the bolt heads of the fasteners that fasten the urban bracket to the wall mount..

13. Mount the camera as shown in the illustrations. Do not tighten fully the mounting hardware until the alignment is complete.

Mounting the Camera Brackets to a Wall

Use the instructions to install brackets to a flat surface, such as a wall.

1. Ensure you have the following bracket components for each camera:

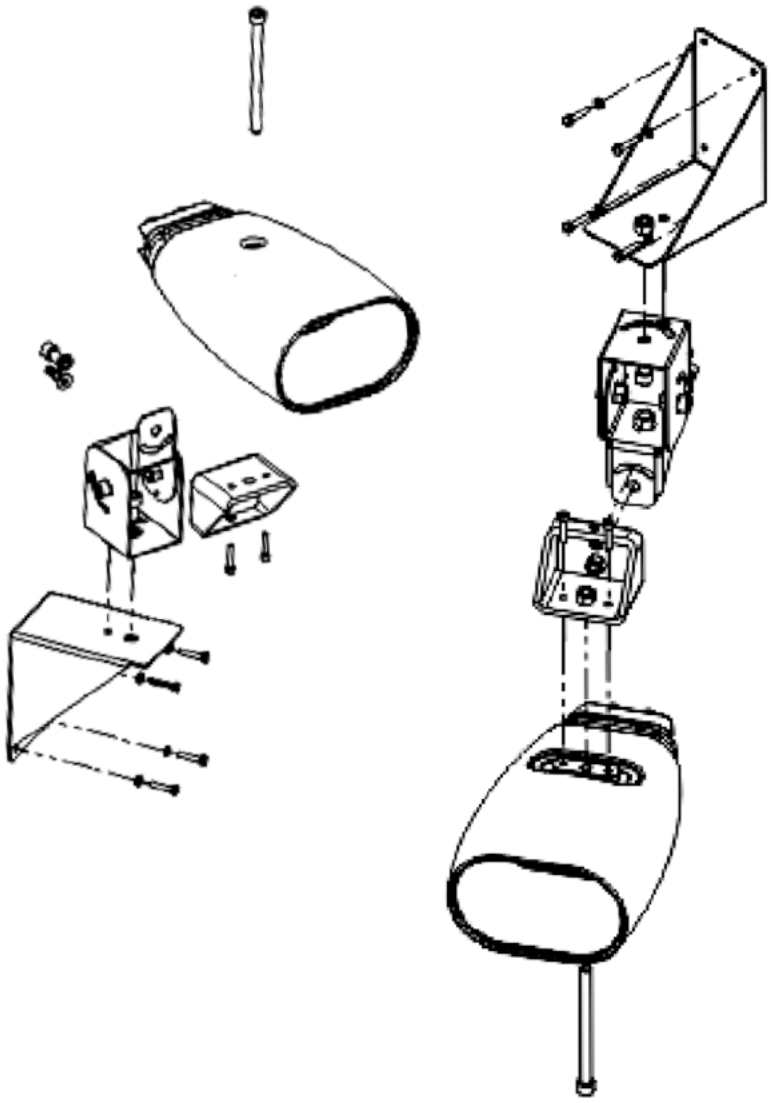
   - Urban bracket
   - Wall bracket

2. Ensure that you have the following tools with you:

   - Drill
   - Marker
   - Socket wrench
   - Sockets
   - Allen Wrenches
   - Lag screws
   - Carriage bolts

   Note:
   - Assemble the urban bracket to the wall mount bracket on the ground if you are using both elements of bracket system.

3. Mark holes using wall mount bracket as guide for location.
4. Drill appropriate sized holes onto surface.
5. Insert anchors into holes (if needed).
6. Attach the wall mount bracket and urban bracket. Be sure the Nordlock washers are in place between the wall mount bracket and pole bracket.
7. Mount the camera as shown in the illustrations.



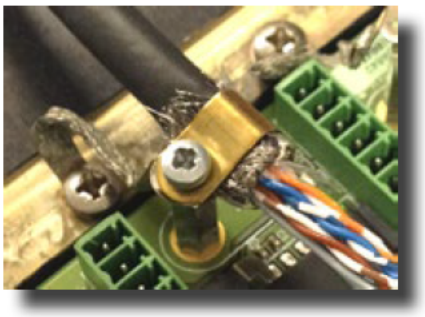
Step 4:Make Camera-Side Cable Connections

Cabling the P382 Camera

1. Open the camera back cover (using a #4 Allen wrench).
2. Insert the cable through the cable gland.
3. Remove approximately 4 in./102 mm from the outer jacket of the cable as shown.
4. Cut the braided shield away from the cable at the jacket:
   - Cut it so that approximately 1/2 in./13 mm is left exposed.
   - Take care not to cut the drain shield wire (Pull the braided shield back for easy cutting).



5. Remove the clear plastic insulation, revealing the paired conductors.
6. Strip all conductors by 1/4 in./6 mm.
7. Apply heat shrink to the drain wire, leaving about 1/4 in./6 mm uncovered.
8. Remove the p-clamp closer to the PL1 connector and snap the clamp around the outside of the cable:
   - Fold the braided shield back over the cable as shown and then snap the clamp around the outside of the cable.
   - Ensure that the clamp is in contact with the braided shield.



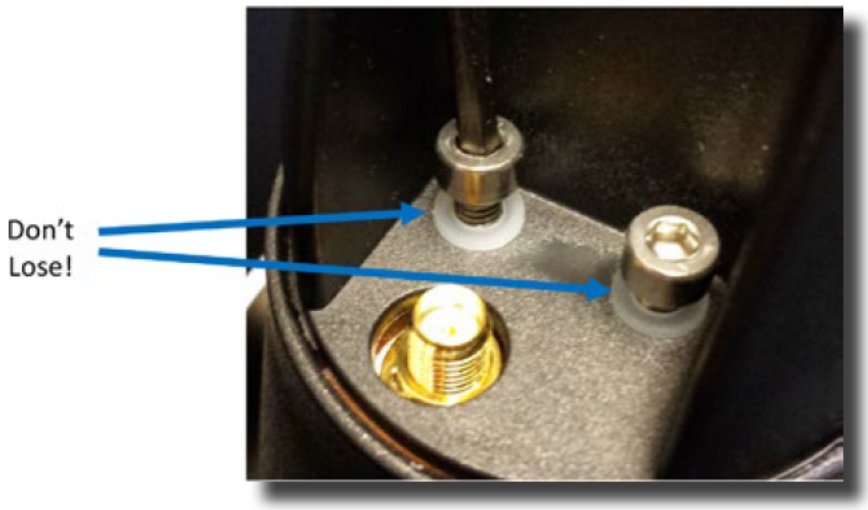
9. Screw the p-clamp back in place, ensuring that the ring tab from the camera braid is under the p-clamp.
10. Screw all conductors to the camera board connectors using the information in the table.

P382 Camera			
Connector	**Pin #**	**Conductor Color**	**Purpose**
P1	12	Pink (lg)	Power
	11	Blue (lg)	Ground
	10	Gray / White	RS-232 GND
	9	Green	RS-232 TX
	8	Green / White	RS-232 RX
	7	Heat shrink color	Drain shield
	4	Orange	Ethernet RX-
	3	Orange / White	Ethernet RX+
	2	Blue	Ethernet TX-
	1	Blue / White	Ethernet TX+
P2	10	Brown	Trigger 2
	9	Brown / White	Trigger 1

11. Screw the back cover of the camera back on and tighten its cable gland (26 in/lbs. max).
12. Run the cable back to camera interface box. Refer to Appendix A for wiring to the interface box.

Cabling the P392+/P492 Camera

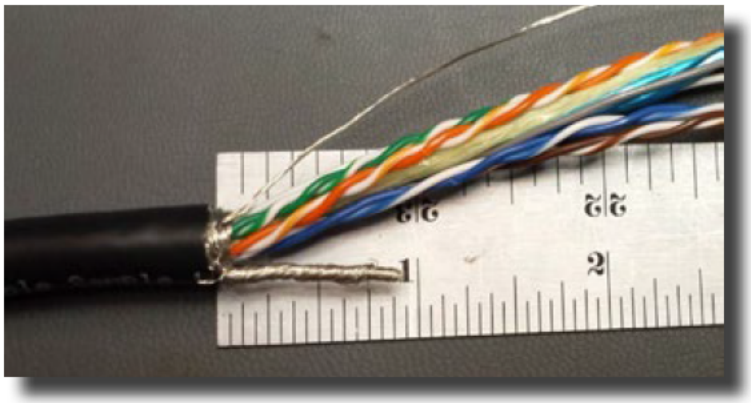
1. Remove the four screws securing the camera back cover using a 3mm hex (Allen) wrench. Be sure not to lose the four nylon washers between the screws and the cover:



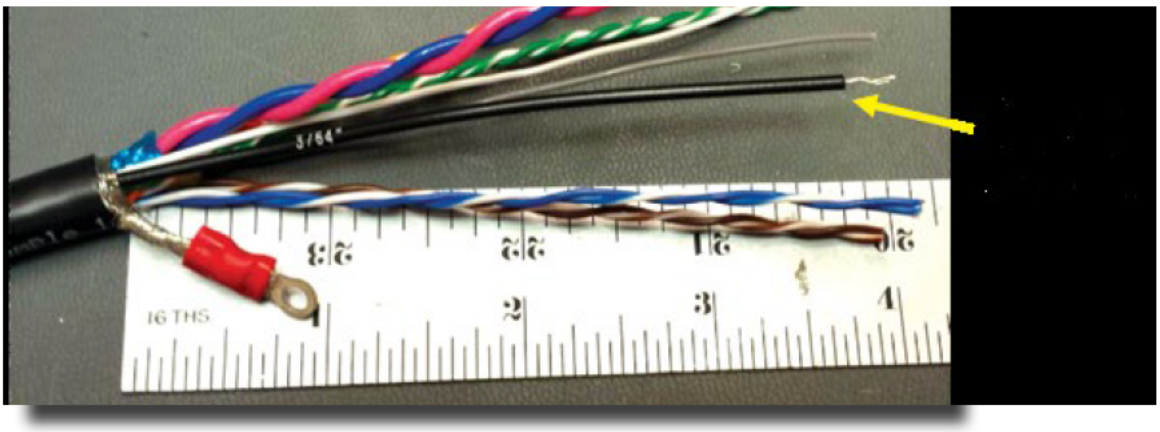
2. Remove about 4" of insulation from the composite cable.



3. Locate the drain wire and fish it out of cable braid near where the outer jacket was cut. DO NOT CUT THE CABLE DRAIN. Cut the cable BRAID back to about 1" and twist:



4. Install a #4, 16-22AWG ring tongue terminal onto the braid. Install about 3 3/4" of 3/64" heat-shrink tubing to the cable drain:



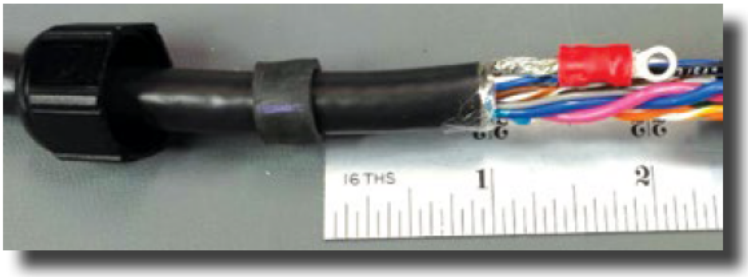
5. Using an 18mm wrench, remove the Cable Gland from the back cover.



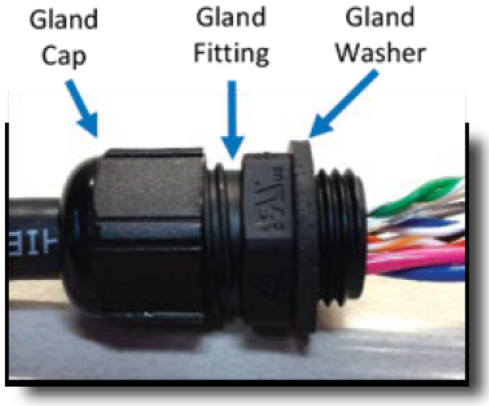
6. Disassemble the cable gland:



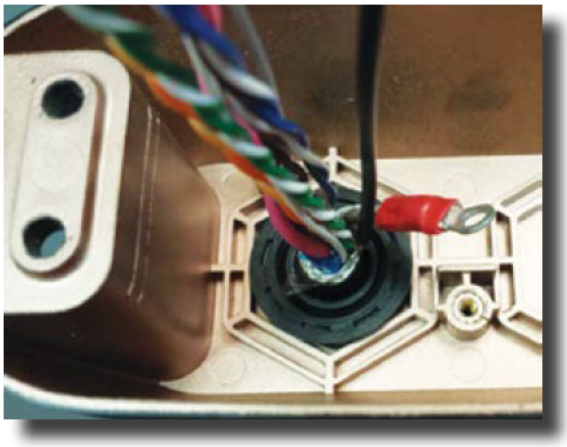
7. Push the composite cable through the Gland Cap first, then the Gland Gasket. Leave about 1" of cable jacket exposed in front of the Gland Gasket.



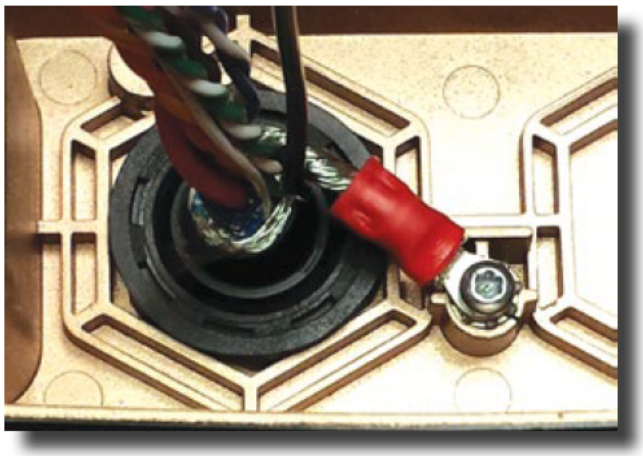
8. Press the fitting over the Gland Gasket by twisting back and forth as you do it. Lightly screw the Gland Cap to the fitting allowing the cable to slide within the fitting. Do NOT tighten the Gland Cap at this time!
   Place the Gland Washer against the Gland Fitting.



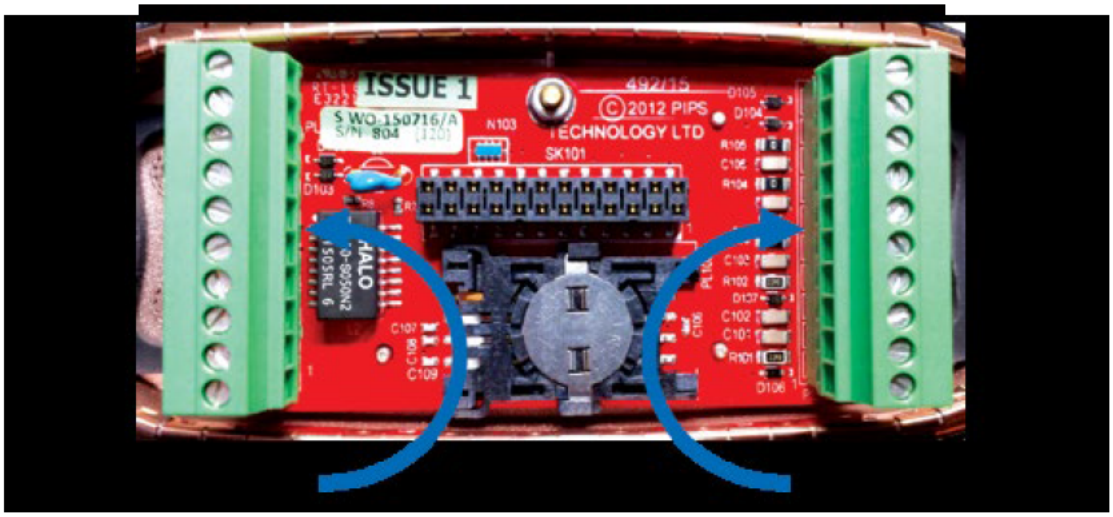
9. Seat the Gland Nut in the hex cavity first on the inside of the back cover. Place the assembled fitting through the back cover by rotating the assembled fitting into the Gland Nut. Tighten with an 18mm wrench.
   Also tighten the gland cap. Do not over-tighten!



10. Using a T10 Torx driver, remove the screw/washers from the back cover. Install the braid wire w/ring tongue terminal to the back cover in this order: torx screw, ring-tongue terminal, star washer, flat washer. Tighten the screw.



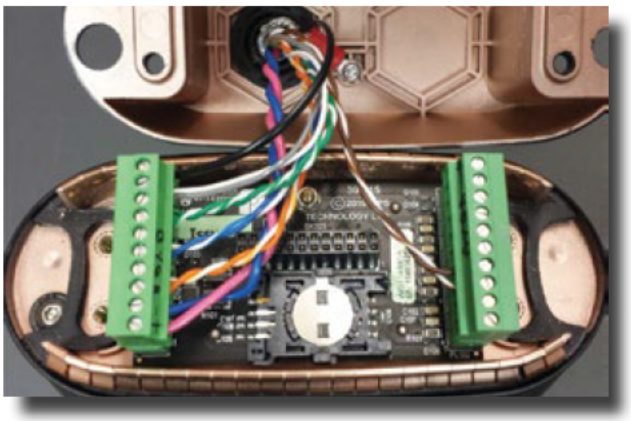
11. Remove the two Phoenix-style connectors from PL101 and PL102 on the camera connector board. Note that regardless of the wire entry to the connectors, pin 1 is always at the bottom of the board:



12. Wire connectors PL101 and PL102 per the table and keep wire pairs twisted right up to the connector body.

P392+/P492 Cameras			
Connector	**Pin #**	**Conductor Color**	**Purpose**
P1	1	Pink (lg)	Power
	2	Blue (lg)	Ground
	3	Orange	Ethernet TX+
	4	Orange / White	Ethernet TX-
	5	Blue	Ethernet RX+
	6	Blue / White	Ethernet RX-
	7	Green / White	RS-232 RX
	8	Green	RS-232 TX
	9	Gray / White	RS-232 GND
	10	Heat shrink color	Drain shield
P2	3	Brown / White	Trigger 2
	4	Brown	Trigger 1

13. Install connectors PL101 and PL102 into the connector board on the back of the camera:

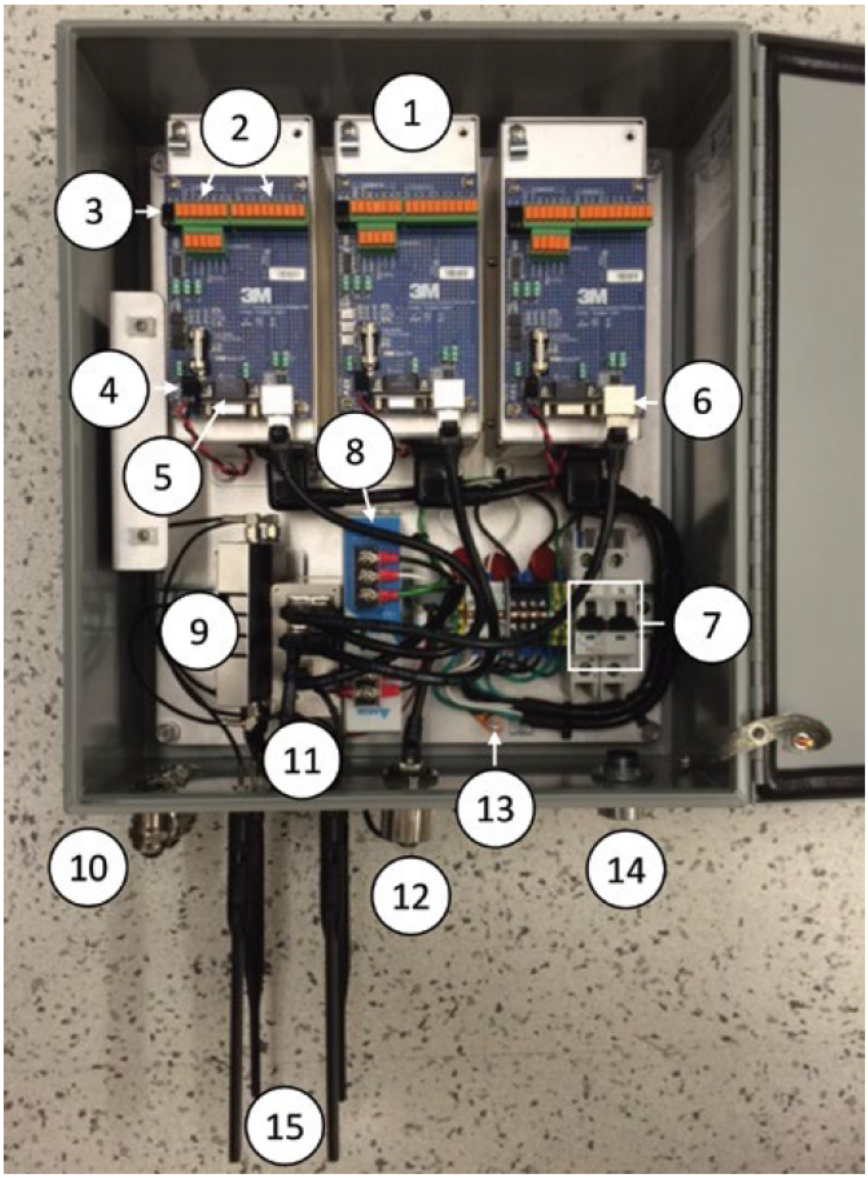


14. Reassemble the back cover with the four screws and nylon washers. Tighten to 0.368 Ft Lbs. / 0.5Nm.

Step 5: Connect the Universal Cable to the Interface Module

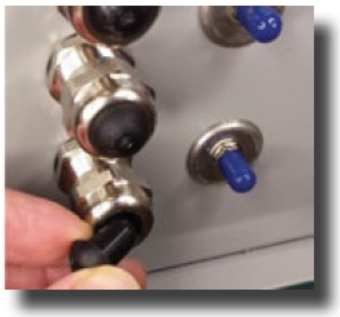
Introduction
A universal cable runs between each camera and an interface module in the camera Interface box.

1. Camera Interface Module (CIM)
2. Camera Comms Connectors
3. Camera Power Connector
4. CIM Output Voltage
5. RS-232 Jack
6. CIM Ethernet Port
7. Power On/Off
8. Ethernet Switch/Modem Pwr (12V)
9. Modem Assembly
10. Cable Glands
11. Ethernet Switch
12. Ethernet Port
13. Earth/Ground Lug
14. Power Entry Conduit Hub (1/2")
15. Modem Antennae



1) Use a crescent wrench to loosen the outer gland nut to remove the gland plug:





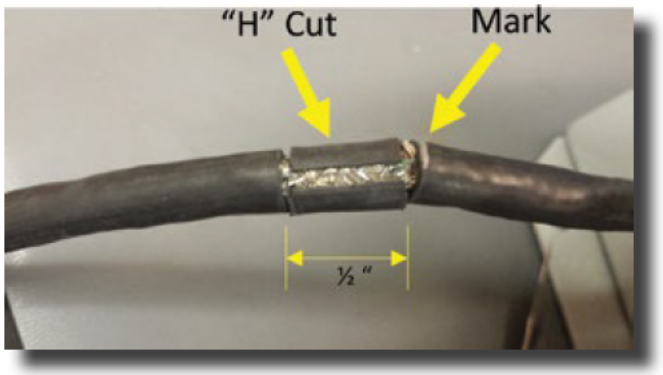
2) Feed the cable through the gland. Route it through the path it will take to the target interface board plus an inch or so:




3) Make a mark on the cable right where it exits the gland:



4) Pull the cable back out of the gland a bit and make an “H” cut on the cable jacket about 1/2” wide. Take care not to cut the braid underneath. Remove this piece of jacket:





5) Push the cable back into the gland and line up the mark on the cable with the back of the gland:



(View from inside the enclosure)

6) Using a crescent wrench, tighten the gland so that the stain relief at the front of the gland compresses around the cable jacket (36 in/lbs. max) and the 360° shield engages the cable braid. Use an ohm meter to verify that the metal of the cable gland has continuity to the cable braid.



(View from outside the enclosure)

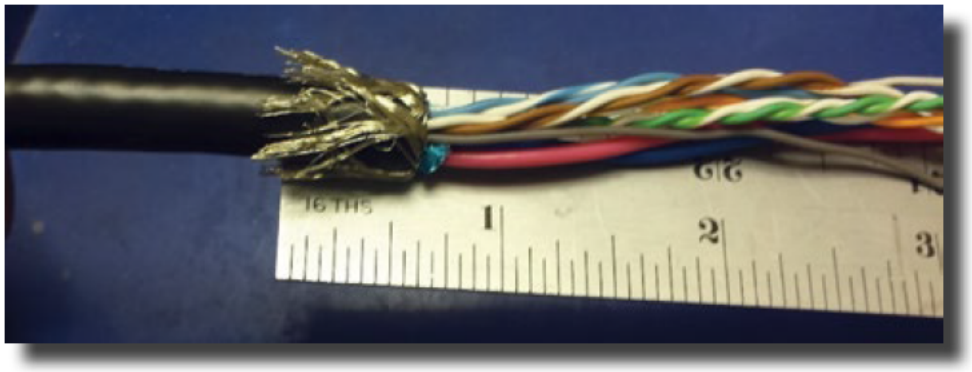
7) Remove 4" of the cable jacket from the end of the cable:



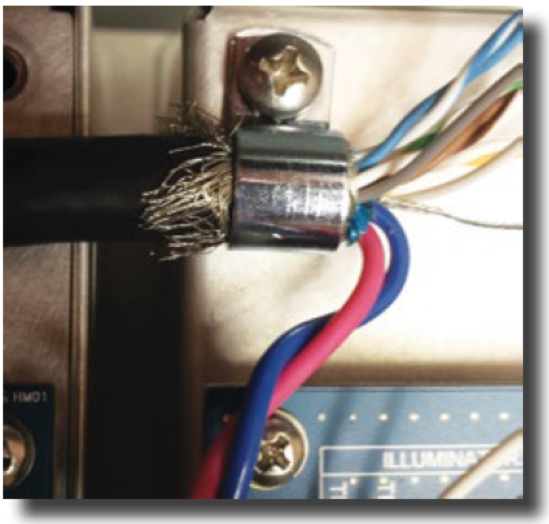
8) Cut and remove the cable braid about 3/4" from where the cable jacket ends.
Take care not to cut the drain wire as it looks like cable braid:



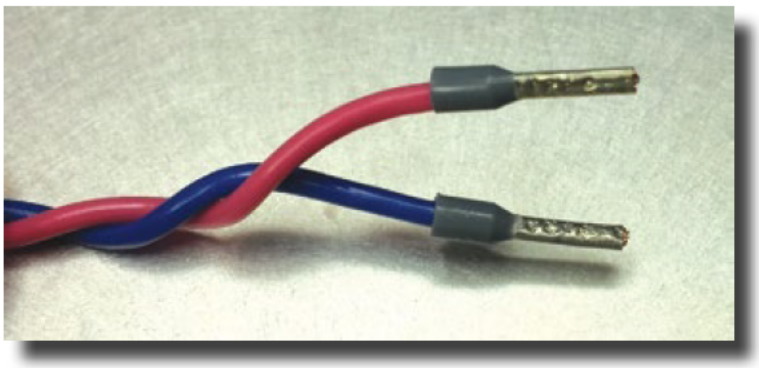
9) Fold the braid back onto the jacket:



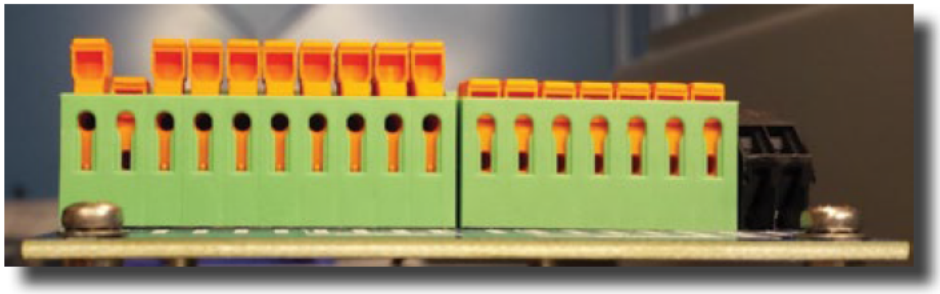
10) Remove the cable clamp from the top of the power supply module, spread it open, place it over where the braid is folded over the jacket and install back onto the power supply module:



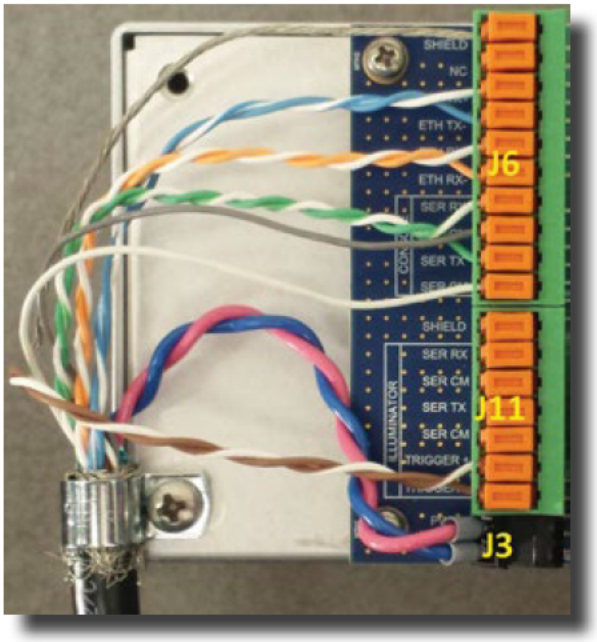
11) Remove about 1/4" of insulation from the larger pink and blue wires (do not remove insulation from the rest of the wires) and crimp an 18AWG wire ferrule to the end of these wires. Twist these wires:



12) Lift, but do not remove the wire latches on the connectors:



13) Do not strip any insulation from the smaller wires. Insert each wire from the cable into the latches until they bottom out. Push the latch down until a firm “click” is felt. Wire as shown in the picture and table:



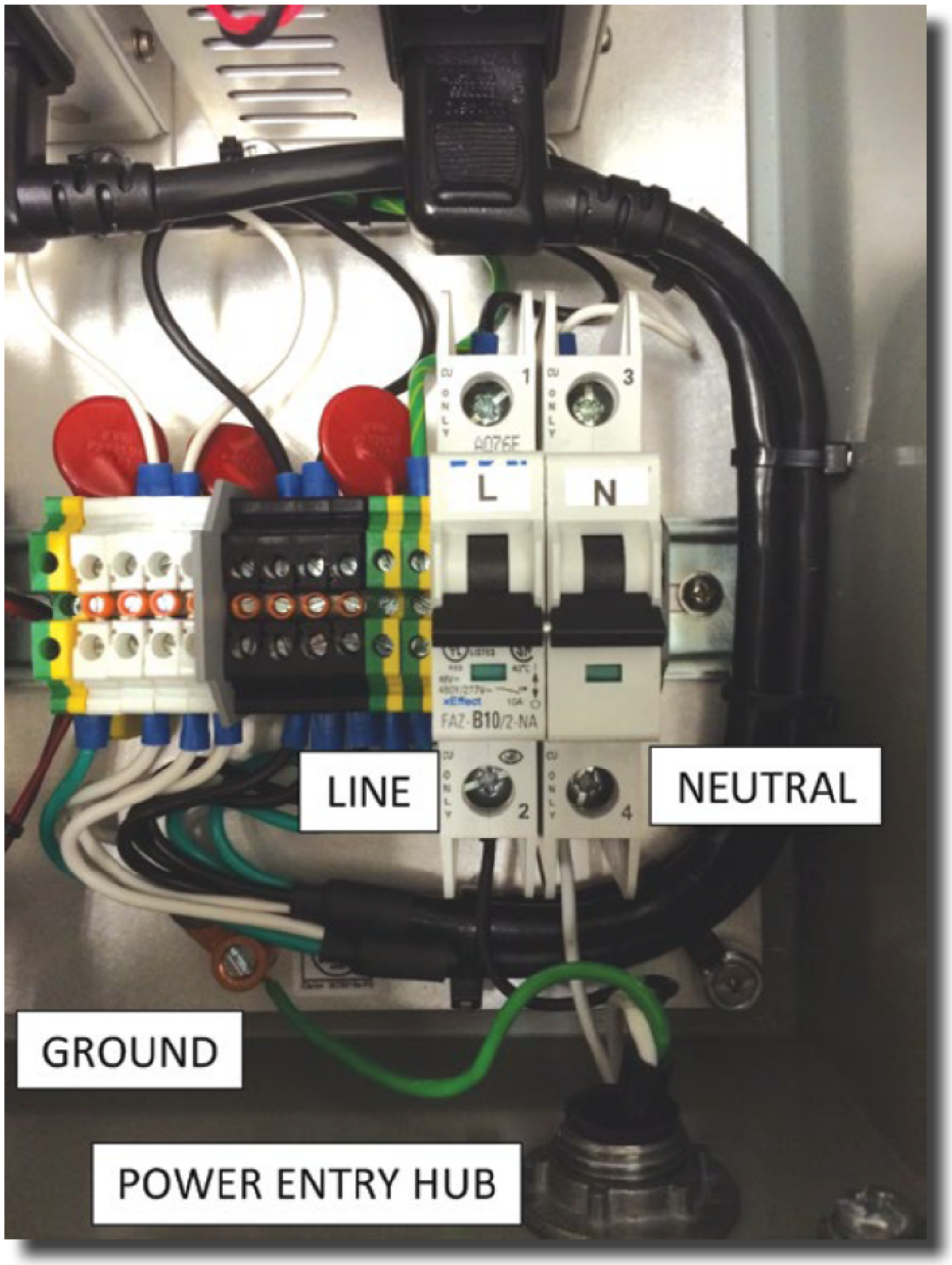
Wiring for P392+/P492 cameras			
Wire Color		CONNECTOR	Label
Drain		J6.1	SHIELD
Blue	White	J6.3	ETH TX+
Blue		J6.4	ETH TX-
Orange	White	J6.5	ETH RX+
Orange		J6.6	ETH RX-
Green	White	J6.7	SER RX
Gray		J6.8	SER CM
Green		J6.9	SER TX
White		J6.10	SER CM
Brown	White	J11.6	Trigger +
Brown		J11.7	Trigger -
Pink		J3.1	PWR +
Blue		J3.2	PWR -
See Appendix A for wiring a P382 camera.			

14) When all camera cables have been routed and connected to the boards on the power supply modules, use two tie wraps to secure the cables to the cable bracket:



Step 6: Connect the Camera Interface Box to the Main

1. Cable selection should always be per local electrical code. As a minimum, 14 AWG, stranded or solid copper conductor, 300V, 90°C rated, is suggested. If stranded wire is selected, use of appropriate wire ferrules are also recommended.
2. Run the cable from the electrical main through the power entry hub (1/2" conduit) at the bottom of the unit.
3. Connect wires as shown and secure tightly.

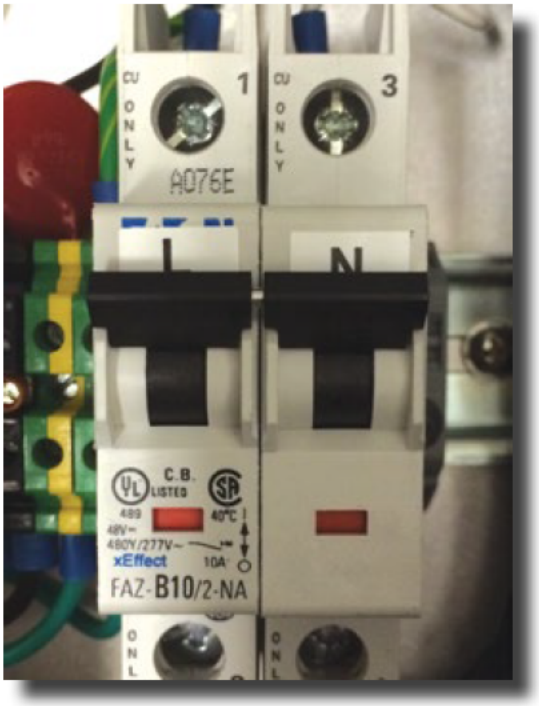


Tightening torque for the line, neutral and ground connections are per the selected wire gauge:

18-12 AWG 21	in/lbs. max
10-8 AWG 25	in/lbs. max
6 AWG 36	in/lbs. max

Step 7: Power on the Camera Interface Box

To power on the camera interface box, flip the power and ground breakers.



Step 8:Configure Network Settings on Your Laptop

This procedure shows you how to configure networking settings on your laptop for communication with the camera. It shows you how to configure the network interface for a second IP address and mask, which will allow communication with the camera without disturbing your laptop's normal network settings.

1. Ensure that you are using static IP addressing.
2. In the Control Panel go to Network and Sharing Center > Change adapter settings.
3. Right click your network adapter and choose Properties.
4. Double-click Internet Protocol (IPv4) and then click Advanced.
5. Add an IP address for communication with the camera, which is configured by default to use a network mask of 255.255.255.0 and an IP address of 192.168.200.201.

Step 9: Set up a Connection to the Customer's Network

There are two ways to connect the camera system to customer's network, depending on the networking equipment in the camera interface box:

- Using wired Ethernet (covered below)
- Using the Cradlepoint modem (See Connecting Using the Cradlepoint Modem on page 36.

Connecting Using Ethernet

Follow the steps below to connect an Ethernet cable.

1. Slide the cable through the connectors as shown.



2. Use the RJ45 crimping tool to connect the RJ45 connector to the cable.



3. Insert the connector into the Ethernet port.
4. Secure the connection by tightening the connector.
5. Power on the camera interface box if required.





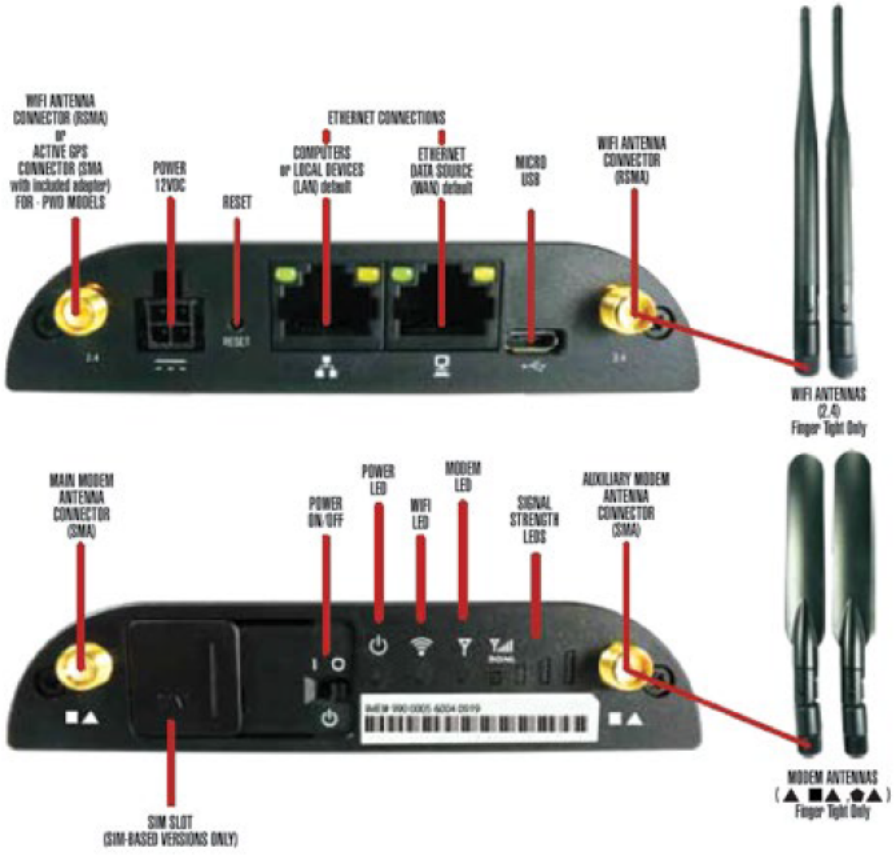
Connecting Using the Cradlepoint Modem

1. Locate and record the following information from the modem label:
   - The unique password for this modem
   - The default SSID password, which is IBR600-xxx, where xxx is the last three digits of the modem's MAC address.



2. Connect antennas as shown.
3. Power on the Camera Interface Box.
4. Connect your laptop to the Ethernet port on the Cradlepoint modem using an Ethernet crossover cable.
5. Start a browser and enter the following in the address bar: cp/ or 192.168.0.1
6. When prompted, enter the password you recorded earlier.
7. When you are directed to the first time set up wizard (first time logging in only) follow the steps to establish a customized wireless network name, password, and security level.

Note: If you are currently using the IBR600 WiFi network, you will need to reconnect your devices to the network using the newly established wireless network name and wireless security password.

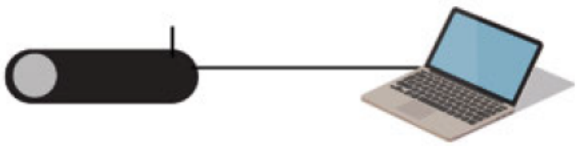


Disconnect your laptop and connect the Ethernet cable to the Ethernet port on the modem.

Step 10: Set up Cameras with the Toolkit

Step A: Connect to the Cameras

1. Connect your laptop to the Ethernet port on the camera interface box's switch **cable using a CAT 5 cable**.



2. Open the Toolkit software.

   The user interface will appear.

3. When the discovery window appears, select the IP address of the laptop's NIC in the dropdown window.
The PIPS™ Toolkit will automatically discover the camera.

Step B: Change the Camera TCP/IP Settings

Note: Pictures in the section show example settings only. Use the correct settings required for your network.

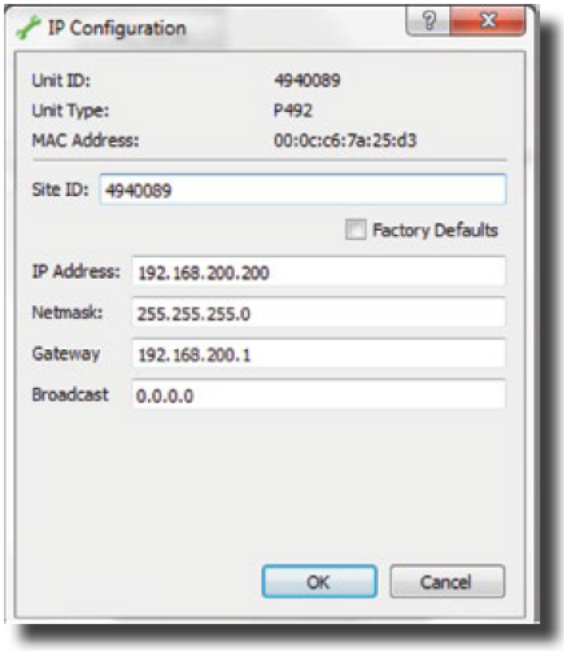
Change the TCP/IP settings by doing the following:

1. In the discovery window, click the camera's "Change IP Address" box.



2. Configure the IP address, network mask, and gateway to appropriate values and then click OK.

   Note: Each camera requires a unique, static IP address.



Step C: Inverting the P392+/P492 Video

The P392+/P492 cameras ship configured to sit on top of the urban bracket. If the camera is hanging underneath the bracket, change the default setting by doing the following:

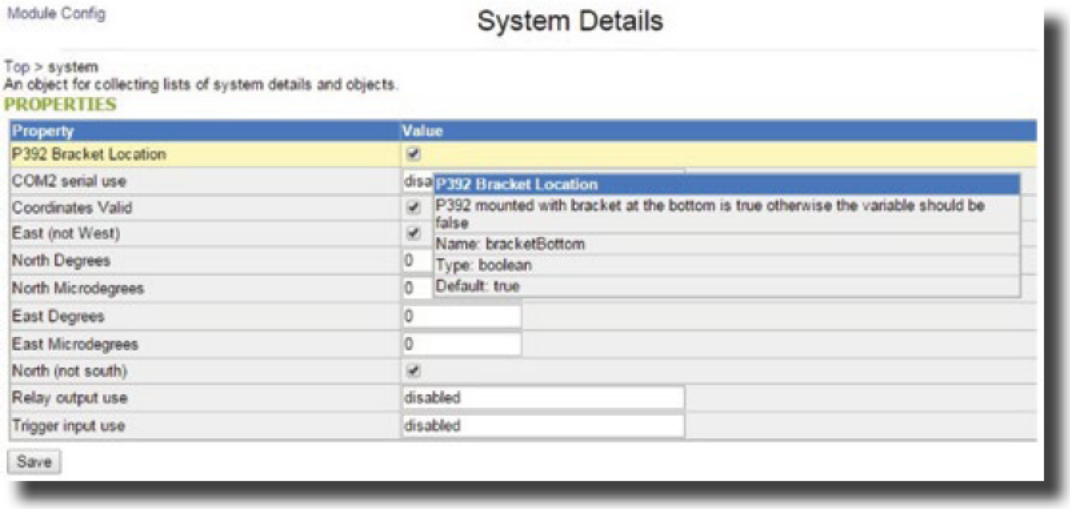
1. Access the Camera web interface by doing one of the following:
- Select the Configuration button on the Toolkit interface.
- Enter the camera's IP address into the browser's address bar in the form: https://ip address/
- Accept the security warning to proceed to the login screen.

2. Log in using the following credentials:
- Username = root
- Password = 382 for P382 cameras or 392 for both the P392+ and P492 cameras



3. Click the "System Details" link in the center of the screen.

4. Uncheck the P392+ "Bracket Location" and then click "Save."



Step C: Inverting the P392+/P492 Video
Goal

There are three thing to look for when aligning the camera.

- Vehicles pass through the field of view of the camera.
- Plates are at the correct distance to stay in focus. This will also ensure they are the correct size. Using the toolkit you can check that the plates are around 140 to 160 pixels wide for US style plates or 180 to 200 pixels wide for the rest of the world.
- Plates are horizontal in the field of view. The top and bottom of the plate must be horizontal, but the sides may be at an angle; this is not a problem.

Procedure for alignment when traffic lanes are closed

Use this procedure for aligning the camera when traffic lanes are closed. To align cameras when lane closure is not possible, see Procedure for alignment when traffic lanes cannot be closed on page 40.

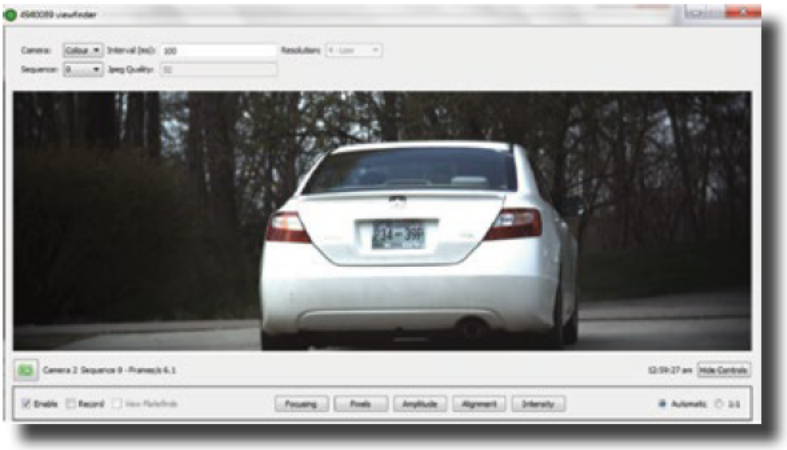
The procedure for aiming the PIPS™ fixed ALPR camera is the same regardless of the camera model. All PIPS™ fixed ALPR cameras are shipped from the factory focused to a specific distance. This distance is critical for properly aiming the camera.

The PIPS™ Toolkit has a 'Viewfinder' utility which is used to aim the camera. The universal fixed camera bracket has three axis of rotation, which are used to center and 'straighten' the license plate in the field of view.

1. If you have not done so already:
   a) Configure the laptop's TCP/IP settings to be compatible with the camera's TCP/IP settings.
   b) Open the PIPS™ Toolkit.
   2. Open the Viewfinder utility by clicking on the camera icon.

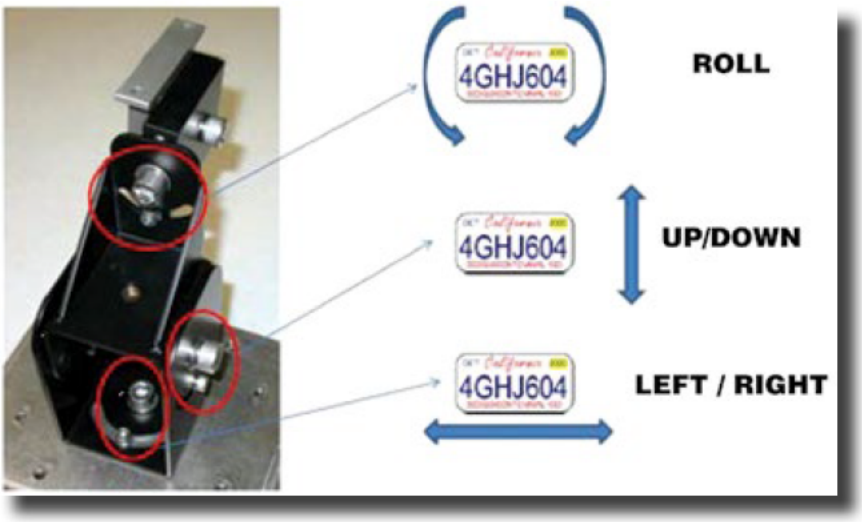
3. Configure the Viewfinder utility to use the color camera at an interval of 100 ms. The color camera is used to do a coarse aiming of the camera.

4. Using a 100 ft. (30 m) tape measure, position a license plate in the center of the lane. Have the installer hold the end of the tape at the camera window and place the license plate at the appropriate focal distance.



5. Using the three axis of rotation in the universal fixed camera bracket, place the license plate in the center of the field of view and parallel (straight) to the camera's horizontal field of view.

6. Snug the alignment bolts.

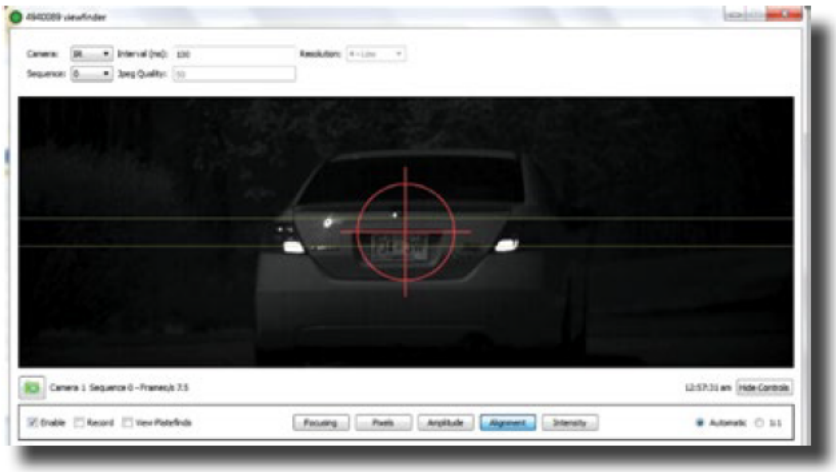


7. Configure the Viewfinder utility to use the IR camera at an interval of 100 ms. The IR camera is used to do the precise aiming of the camera.

8. Using the three axis of rotation in the universal fixed camera bracket, place the license plate in the center of the field of view and parallel (straight) to the camera's horizontal field of view.

9. Tighten alignment bolts.

10. Confirm license plate is still center and straight in the field of view.



Procedure for alignment when traffic lanes cannot be closed

Because alignment with live traffic is difficult, contact PIPS™ before attempting this procedure.

Chapter 7.
Camera Maintenance

The camera is designed to minimize maintenance, so maintenance tasks are minimal. It is recommended that you check and clean the camera every six months.
Maintenance tasks include the following:

- Cleaning the front window of the camera with clean water and a lint free cloth. If you have very hard water, you may find de-ionised water helps prevent streaking. You can use a small amount of detergent if you have grease on the lens.
- Checking inside the camera's hood for any foreign objects and remove them.
- Checking the camera for alignment. You may wish to perform a site acceptance test (SAT) to check performance.
- Checking and tighten all brackets, fittings and cables.
- Checking the bracket, camera, cables and power supply for damage or wear and replace as necessary.
- Checking that communications links to and from the camera work as expected.

Appendix A. Cabling Reference

Camera Side

P382 Camera			
Connector	Pin #	Conductor Color	Purpose
P1	12	Pink (lg)	Power
	11	Blue (lg)	Ground
	10	Gray / White	RS-232 GND
	9	Green	RS-232 TX
	8	Green / White	RS-232 RX
	7	Heat Shrink Color	Drain shield
	4	Orange	Ethernet RX-
	3	Orange / White	Ethernet RX+
	2	Blue	Ethernet TX-
	1	Blue / White	Ethernet TX+
P2	3	Brown	Trigger 2
	4	Brown / White	Trigger 1

P392+/P492 Cameras			
Connector	Pin #	Conductor Color	Purpose
P1	1	Pink (lg)	Power
	2	Blue (lg)	Ground
	3	Orange	Ethernet TX+
	4	Orange / White	Ethernet TX-
	5	Blue	Ethernet RX+
	6	Blue / White	Ethernet RX-
	7	Green / White	RS-232 RX
	8	Green	RS-232 TX
	9	Gray / White	RS-232 GND
	10	Heat shrink color	Drain shield
P2	3	Brown / White	Trigger 2
	4	Brown	Trigger 1

Interface Box Side

P382 Camera		
Conductor Color	CONNECTOR	Label
Drain	J6.1	SHIELD
Blue / White	J6.3	ETH TX+
Blue	J6.4	ETH TX-
Orange / White	J6.5	ETH RX+
Orange	J6.6	ETH RX-
Green / White	J6.7	SER RX
Gray	J6.8	SER CM
Green	J6.9	SER TX
White	J6.10	SER CM
Brown / White	J11.6	Trigger +
Brown	J11.7	Trigger -
Pink	J3.1	PWR +
Blue	J3.2	PWR -

P392+/P492 cameras		
Conductor Color	CONNECTOR	Label
Drain	J6.1	SHIELD
Blue / White	J6.3	ETH TX+
Blue	J6.4	ETH TX-
Orange / White	J6.5	ETH RX+
Orange	J6.6	ETH RX-
Green / White	J6.7	SER RX
Gray	J6.8	SER CM
Green	J6.9	SER TX
White	J6.10	SER CM
Brown / White	J11.6	Trigger +
Brown	J11.7	Trigger -
Pink	J3.1	PWR +
Blue	J3.2	PWR -

Appendix B. RS-232 Default Settings

These are the default settings for the camera's RS-232 interface:

- 38,400 bps
- 8 bits
- No parity
- 1 stop bit

Appendix C. Firewall Settings

To enable remote access to the camera, the customer's network firewall must permit all the TCP port numbers listed below.

- 22 (SSH)
- 443 (HTTPS)
- 3570 (Event Viewer)
- 3820 (Trigger)
- 9000 (Viewfinder)

The firewall must also permit Ethernet type 0xAC01.

Note: To upgrade the camera firmware, the Toolkit will act as a TFTP and DHCP server. The firewall must allow this to happen.

Appendix D. Product Warranty

PRODUCT USE STATEMENT

Product Use: Many factors beyond PIPS™ control and uniquely within user's knowledge and control can affect the use and performance of a PIPS™ product in a particular application Given the variety of factors that can affect the use and performance of a PIPS™ product, user is solely responsible for evaluating the PIPS™ product and determining whether it is fit for a particular purpose and suitable for user's method of application.

Warranty, Limited Remedy, and Disclaimer: Many factors beyond PIPS™ control and uniquely within user's knowledge and control can affect the use and performance of a PIPS™ product in a particular application. User is solely responsible for evaluating the PIPS™ product and determining whether it is fit for a particular purpose and suitable for user's method of application. Unless a different warranty is specifically stated on the applicable PIPS™ product packaging, product literature, terms of sale or software license agreement, PIPS™ warrants that (i) the PIPS™ product will be free from substantial defects in material and workmanship under normal use and service, wear and tear excepted, for twelve (12) months from the date of shipment, and (ii) for software products, for twelve (12) months from the date of shipment, the software will materially perform the functions described in the accompanying documentation. PIPS™ MAKES NO OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR ANY IMPLIED WARRANTY OR CONDITION ARISING OUT OF A COURSE OF DEALING, CUSTOM OR USAGE OF TRADE. If the PIPS™ product does not conform to this warranty, then the sole and exclusive remedy is, at PIPS™ option, repair or replacement of the PIPS™ product or refund of the purchase price.

Limitation of Liability: Except where prohibited by law, PIPS™ will not be liable for any loss or damage arising from the PIPS™ product, whether direct, indirect, special, incidental or consequential, regardless of the legal theory asserted, including warranty, contract, negligence or strict liability.

Disclaimer: Use of system components (cables, power supplies, connectors, fasteners, or support brackets) other than those recommended by PIPS™, may compromise product performance, will invalidate PIPS™ EMC (Electromagnetic Compatibility) and safety certifications and voids PIPS™ warranty.

For additional information, assistance or maintenance questions please contact Neology ALPR/ANPR Support at:

PHONE: 833-PIPS-LPR (833-747-7577)
- **Option 1 for Sales**
- **Option 2 for Support**

For the U.S/Can and all other areas:
Sales Enquiry Email: sales@pipstechnology.com
Support Request Email: support@pipstechnology.com

For Europe, Middle East and Africa:
Sales Enquiry Email: sales@pipstechnology.co.uk
Support Request Email: support@pipstechnology.co.uk

PIPS TECHNOLOGY DETECTION INNOVATION
IS A TRADEMARK OF NEOLOGY INC., AND EITHER REGISTERED OR PENDING REGISTRATION IN SEVERAL JURISDICTIONS.

Neology Headquarters San Diego
Address: 12760 Danielson Ct.,
Suite A Poway, CA 92064

Neology UK Ltd
Address:Form 1 Bartley Wood Business Park
Hook, Hampshire
RG27 9UP

Neology México
Plaza Carso II, Lago Zurich No. 219-Piso 10
C.P. 11529 Ciudad de México

NEOLOGY MOBILITY TECHNOLOGIES

AutoVu SharpZ3

Mobile Automatic License Plate Recognition System

High performance and edge-based mobile ALPR

The AutoVu™ SharpZ3 is a mobile automatic license plate recognition (ALPR) system that goes beyond traditional plate identification. It brings new levels of insight in vehicle analytics, situational awareness, and accuracy.

That's because the SharpZ3 is powered by the latest edge-based processing technology. Designed to combine high-performance and low power consumption, it lets you take full advantage of machine learning capabilities directly at the edge. And with its third optical sensor, the SharpZ3 can precisely position objects and vehicles to understand what's around the license plate, placing reads into context.

Expand your vision with the AutoVu SharpZ3.

Features

- Powered by AutoVu MLC machine learning based engine
- Built-in vehicle type, color and plate origin recognition analytics
- Ultra-low reading latency
- 3 optical sensors
- Modular architecture designed to evolve seamlessly
- Optional advanced GPS positioning with dead reckoning
- Up to 4 high-definition ALPR cameras on the same base unit
- Unified with Genetec Security Center





Get more from your mobile ALPR system

Go beyond conventional mobile ALPR

With the latest neural networking technology built in, the SharpZ3 redefines what mobile ALPR can do. Not only does it deliver higher accuracy and reduce misreads, the SharpZ3 unlocks new insights through its expanded suite of vehicle analytics.

Capture the full picture

With its third optical sensor, the SharpZ3 effortlessly navigates complex urban environments. From flat and non-reflective plates to embossed designs and digital plates, the SharpZ3 can detect more plate designs than traditional units.

Evolve your system with ease

The SharpZ3 is designed with growth in mind. The modular chassis of the SharpZ3 will protect your investment and let you tap into new modules and capabilities over time. This reduces the complication and cost of hardware replacement.

AutoVu SharpZ3 Camera Specifications

ALPR camera sensors
1456(H) x 1088(V) progressive scan @30fps, monochrome, global shutter

ALPR capture range
Up to 63-foot (19-meter) range with retro-reflective license plates

ALPR camera lens options
8mm, 12mm, 16mm, 25mm

Context camera sensor
1456(H) x 1088(V) progressive scan @30fps, color, B&W night mode with 940nm illuminator, global shutter. JPEG still images and MJPEG video streaming

Context camera lens
Based on ALPR lens configuration: (4mm, 6mm, 8mm, 12mm)

Illuminators
Pulsed LED illuminator (740nm, 850nm, 940nm, 590nm)

Water-resistance | sealing
IEC 60529 IPx6, IPx7 | IEC 60529 IP6x

Dimensions
1.65 (h) x 5.12 (w) x 3.56 (d) inches (4.2 × 13 × 9 cm) | Excludes cabling and mounting bracket

Weight
1.2 lbs (0.54kg)

Color
Available in black/white

AutoVu SharpZ3 Base Unit Specifications

I/O
Base unit:
2x 10/100/1000 Base-T Ethernet ports (RJ45)
4x digital inputs (triggers), 0~32Vdc, opto-coupled
4x dry-contact outputs (relays): 2x 0.25A solid state relays, 2x 8A electromechanical relays
1x regulated 12V AUX output power, 200mA

Mounting options
Horizontal and vertical

Dimensions
3.6 (h) x 8.6 (w) x 9.3 (d) inches (9.1 × 21.8 × 23.6 cm).
Excludes cabling, cable racks and mounting brackets

Weight
Base unit: 4.4 lbs (2.0 kg)
ALPR module: 2-ports: 4.1 lbs (1.9 kg)
ALPR module: 4-ports: 4.4 lbs (2.0 kg)

Processors
Intel Atom Processor E3950
Additional dedicated machine-learning co-processor

Power
12/24Vdc nominal (9 to 32 Vdc)
Optional modules:
2x ALPR unit base module
Typical Power consumption: 50W (with cameras)
4x ALPR unit base module
Typical Power consumption: 98W (with cameras)

AutoVu SharpZ3 System Certification (Camera + Base unit)

Vibration
IEC 60068-2-64

Shock resistance
IEC 60068-2-27

Electromagnetic immunity & emissions
FCC part 15 Sub-part B | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR24 / EN55024 | CISPR25 / EN55025 | EN 50498

CE marking
EMC Directive 2014/30/EU; Automotive EMC Directive 2004/104/EC; RoHS Directive 2011/65/EU (including EU Directive 2015/863)

Temperature
-40°F to 131°F (-40°C to 55°C) operating; -40°F to 185°F (-40°C to 85°C) storage
-40°F to 149°F (-40°C to 65°C) base unit operating, w/optional cooling pack
Certifications: IEC 60068-2-1 Category Ad and Ae | IEC 60068-2-2 Category Be | IEC 60068-2-14 Category Na
Includes hi-temp auto-shutoff protection

Optional modules

PoE module

Function
Connect up to 4 PoE devices

Ports
4x 10/100/1000 Base-T ethernet ports with ix Industrial(tm) connectors
PoE+ capable - 802.3at Type 2 (30.0W)

Power
60W total power budget for powered devices

Navigation module

Function
Integrated inertial sensors with automotive dead reckoning

Connectivity
Multi-constellation single-band (L1) GNSS receiver (GPS/Galileo/GLONASS)
VSS and odometry sensor inputs for wheel ticks

Auxiliary camera

Function
Auxiliary wheel imaging camera unit

Sensor:
2MP sensor with f4.0 mm lens

Power
PoE 802.3af Type 1 (5.8W)

Iluminators:
Built-in IR illumination

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2020. Genetec, AutoVu and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

UPDT-JUL14-20

GUARDIAN

A Publication of the Commercial Vehicle Safety Alliance

Volume 29, Issue 1
1st Quarter 2022



DRUG RECOGNITION EVALUATION POST-INCIDENT REVIEW:

SOMETHING TO CONSIDER IN CASES WITHOUT AN EVALUATION

What to Do If You Suspect a Staged Accident

U.S. DOT Releases Comprehensive National Roadway Safety Strategy

Mexico's SCT Becomes SICT

GUARDIAN
First Quarter
Volume 29, Issue 1
www.cvsa.org

GUARDIAN

IN THIS ISSUE

Insight
President's Message 1
Executive Director's Message 2

Regional News
NJDOT Implements Real-Time Traffic Alert System for Commercial Vehicles 3
Oklahoma's Delaware County Implements Virtual Weigh Station 4
Florida Highway Patrol Conducts Post-Crash Training Course 5
North Carolina State Highway Patrol Commercial Vehicle Enforcement Updates 6
Updates from Mexico 7
Montana Travel Team Saturates Locations and Focuses on Level I Inspections 8

Cover Story
Drug Recognition Evaluation Post-Incident Review: Something to Consider in Cases Without an Evaluation 9

CVSA Committee and Program News
CVSA Welcomes Three New Staff Members 12
CVSA Offers Hazardous Materials Instructor Training 12
Five Reasons Why Fatigue Is a Tough Cookie to Crack 13

Inspector's Corner
Competition 17

Government News
The Legislative and Regulatory Rundown 18
U.S. DOT Provides More than $27 Billion to Fix Bridges Nationwide 19
FMCSA Creates Brochure on Recording the Correct Driver's License Number for CMV Drivers From Mexico or Canada 20
FMCSA Registration Overview 20
U.S. Bureau of Transportation Statistics Announces a Vehicle Inventory and Use Survey 21
U.S. Department of Transportation Releases Comprehensive National Roadway Safety Strategy 22

Knowledge Matters
While the Country Slowed Down, Drivers Sped Up: What This Means for Teens 26
How the National Transportation Safety Board "Most Wanted List" Can Make Our Roads Safer 28
What to Do If You Suspect a Staged Accident 29
How Carriers Can Lead with Lagging Indicators 30
Training, Research and Education for Driving Safety Program Offers Train the Trainer Workshops to Increase Driving Safety Awareness and Decrease Distracting Driving Behaviors Among Commercial Drivers 31

From the Driver's Seat
Winter Weather Can Be Messy 32

Industry Perspectives
Avoid Wheel-Offs with Proper Wheel Maintenance 33
Addressing the Nation's Driver Shortage by Cultivating a Driver-First Safety Mindset 34
Kodiak Robotics Names Brett Fabbri as Head of Law Enforcement Policy and Roadway Safety 35

RAD Inspection News
Waste Isolation Pilot Plant 2021, at a Glance 36
Waste Isolation Pilot Plant Receives 13,000th Shipment 37
2022 Level VI Certification Training Schedule 37
Longtime Level VI Inspection Program Advocate Gaylon Fuller Passes Away 38
Level VI Roadside Inspections (2022 - Fiscal) 38
Level VI Roadside Inspection Violations (2022 - Fiscal) 38

GUARDIAN
"Guardian" is published quarterly by the Commercial Vehicle Safety Alliance with support from the Federal Motor Carrier Safety Administration. CVSA and FMCSA are dedicated to the government and industry working together to promote commercial motor vehicle safety on North American highways.

Phone: 301-830-6143 • Website: www.cvsa.org

CVSA Staff: Collin B. Mooney, MPA, CAE, Executive Director • Adrienne Gildea, CAE, Deputy Executive Director • Carlisle Smith, Director of Level VI Inspection Program • William Schaefer, Director of Safety Programs • Ken Albrecht, Director of Multimedia Development • Bill Reese, Director of Hazardous Materials Programs • Kerri Wirachowsky, Director of Roadside Inspection Program • Christopher Turner, Esq., Director of Enforcement Data and Judicial Outreach • Terry Kummer, Director of Crash Data and Investigation Standards • Jake Elovirta, Director of Enforcement Programs • Nicole Leandro, Senior Manager of Communications • Iris Leonard, Manager of Member Services • Daniel Zimmerman, Senior Manager of Government Affairs • Amanda Wagner, CMP, Senior Manager of Conference and Event Services • Mark Mills, Multimedia Specialist • Wendy Smith, Learning Management System Specialist • Katie Morton, Hazardous Materials Specialist • Rodolfo Giacoman, Fatigue Management System Specialist • Ariel Carter, Grants Management Specialist • Moniladae Adewoyin, Accountant • Wendy Hall, Administrative Coordinator

Copyright 2022, CVSA. All rights reserved. No part of this issue may be reproduced without written permission from the publisher.

For comments, suggestions or information, email communications@cvsa.org.

Commercial Vehicle Safety Alliance **@CVSA**

This material is based upon work supported by the Federal Motor Carrier Safety Administration under a grant/cooperative agreement/subaward. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the view of the Federal Motor Carrier Safety Administration and/or the U.S. Department of Transportation.



PRESIDENT'S MESSAGE

Consider Leadership

*By **Capt. John Broers**, South Dakota Highway Patrol, CVSA President*

A couple of years ago, I started telling my now 7-year-old nephew "dad jokes." Mostly, these were over the phone or occasional video chat. When the jokes worked — when he got the reference and my timing was on — the laughs and giggles that came from him were contagious. Occasionally, he'd roll his eyes, as only a 7-year-old can, with sheer contempt at how silly he thought some of the jokes were. However, a few of my favorite dad jokes received little to no reaction. They would flow from me with what I thought was perfect execution, followed by eager anticipation of the infectious laugh that I thought was sure to follow but never came. I would repeat the punchline, thinking he just didn't hear it. He sometimes spared none of my feelings with his thoughts on a particular joke; other times, he quickly changed the subject to his favorite superhero.

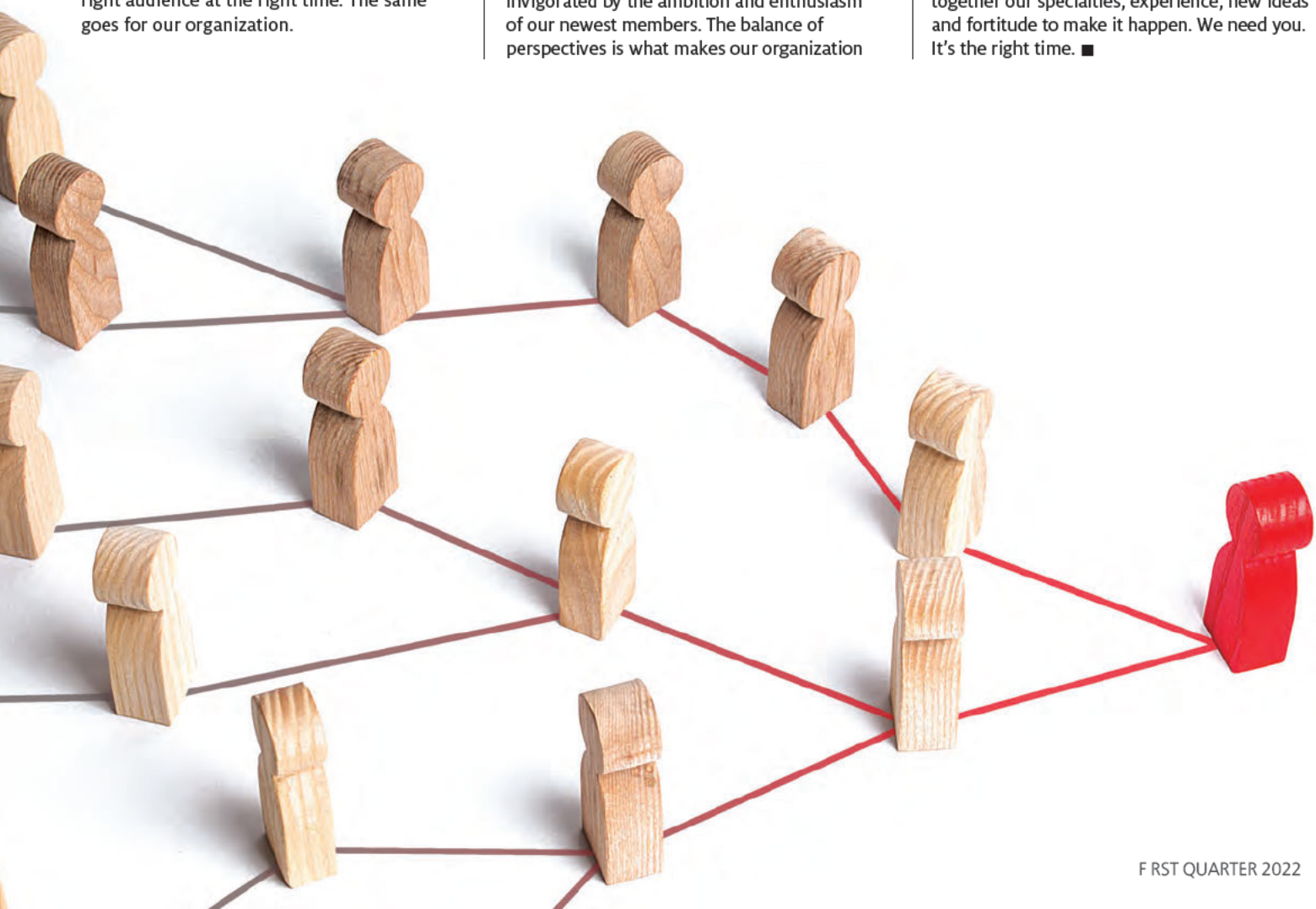
The lesson? The right dad joke works for the right audience at the right time. The same goes for our organization.

The experience that members of the Alliance bring to the organization varies widely. The veterans experienced the beginning of the Alliance and where we came from. They know the "why," the "when" and the "what for." Some of us remember removing worn horseshoes and a broken cinch from the out-of-service criteria. Our newest members may lack some of the historical perspective, but are eager, willing and excited for modernization. Some are curious as to why we aren't inspecting trucks virtually yet. We are all looking forward to the future and what it will bring.

To reach that future successfully, the Alliance needs participation from our next generation of leaders within our membership. Whether your experience is with wagons or the latest technology, the Alliance needs you to move us forward. Our newest members rely on the experience and knowledge of veteran members. In turn, those veterans are invigorated by the ambition and enthusiasm of our newest members. The balance of perspectives is what makes our organization flourish. It's the dad joke that everyone gets; it just works.

So, whether the next conference is your first or your 50th, please consider one of the Alliance's many leadership opportunities. Encourage your coworkers to consider it, too. All it takes is the desire to be part of CVSA's future. We need all kinds of perspectives. We all have our strengths and weaknesses, our priorities and specialties. You don't need to have an agenda, prior leadership experience or endorsements from a superhero. We simply need you and your desire to be part of what comes next for the Alliance. You can start small, in a program, committee or your region.

Leaving your mark on the future of commercial motor vehicle safety is a legacy worth pursuing. The road to zero highway fatalities needs people like you to build it. We need a variety of people working on the project, bringing together our specialties, experience, new ideas and fortitude to make it happen. We need you. It's the right time. ■





EXECUTIVE DIRECTOR'S MESSAGE

The Importance of Effective CVSA-Certified Roadside Inspector Training

*By **Collin B. Mooney**, MPA, CAE, Executive Director, Commercial Vehicle Safety Alliance*

Effective, relevant training is the foundation of a uniform and impactful roadside inspection and enforcement program. In an ever-changing regulatory environment, each new rule or change in regulations requires in-service refresher training to bring seasoned enforcement personnel up to date. Each new exemption provided to the motor carrier industry and the various advancements in vehicle design and technology also necessitate ongoing training. Simply put, enforcement personnel must keep up with the latest industry developments to properly enforce the regulations and standards they are sworn to uphold. This new information must be presented to inspectors clearly, consistently and in a timely manner in order for them to effectively apply it roadside.

This has not been the case under the current process, where inspector training is delegated to a third-party administrator that is not substantively connected to the commercial motor vehicle inspection and enforcement community. For many years, the membership of the Alliance has expressed concerns over the quality of these training services, citing training materials that have not been updated in a timely manner, often containing outdated and inaccurate information. Outdated training leaves many state agencies struggling to ensure their inspectors and enforcement personnel have the information they need to effectively enforce the latest regulations in a consistent and uniform manner.

The problem is compounded when the administrator's lack of technical abilities, subject matter expertise and knowledge of inspection and enforcement practices supplants the dedicated work of the commercial motor vehicle roadside enforcement and inspection community. It makes little sense to continue with this inefficient and ineffective process of delegating inspector training.

As the founding organization and entity responsible for the development and maintenance of all non-regulatory elements of the North American Standard Inspection Program, CVSA is uniquely qualified and well positioned to deliver state roadside inspector training. Over the years, the Alliance has developed the tools and equipment used in the roadside inspection process and has authored and produced the certification standards, inspection procedures, operational policies, inspection bulletins, training videos, safety standards, enforcement tolerances and North American Standard Out-of-Service Criteria referenced throughout the Federal Motor Carrier Safety Regulations (FMCSRs).

Enforcement of the FMCSRs and Hazardous Materials Regulations (HMRs) is a very specialized field that would be better served by the involvement of the organization directly involved in the foundational development and maintenance of the regulations. CVSA's understanding of the regulations, guidance and related policy will enable the Alliance to effectively deliver critical safety training to the enforcement and inspector community in a timely manner. CVSA also shares the Federal Motor Carrier Safety Administration's (FMCSA) commitment to providing the states and territories with the training resources they need to succeed and will do everything possible to make them successful.

The Alliance is a public-sector nonprofit association comprised of local, state, provincial and territorial commercial motor vehicle safety officials. In partnership with FMCSA, the membership of the Alliance has a long history of strong collaboration with all parties working to improve commercial motor vehicle safety. CVSA and FMCSA service the same constituency and, as a result, often work together to help ensure the jurisdictions have the tools and resources needed to reduce crashes, injuries and fatalities on our nation's roadways, while ensuring accurate, uniform enforcement of the FMCSRs and HMRs.

The Alliance has an established history of producing quality training content, playing a leading role in the development and maintenance of all roadside inspection materials for the enforcement community in Canada, Mexico and the United States. Additionally, the Alliance has the technical abilities and subject matter expertise to effectively deliver the necessary training as well. Given that the Alliance is statutorily recognized as the organization that certifies roadside inspection and enforcement personnel to conduct on-road commercial motor vehicle safety inspections, it should be the organization that provides all services related to state inspector training and certification.

Consistency and uniformity in enforcement are the cornerstones of the North American Standard Inspection Program, and the enforcement officials that make up CVSA's core membership are responsible for the day-to-day execution of roadside inspection and enforcement activities. As the organization that represents the roadside inspection community and the entity that founded and maintains the inspection program, the Alliance has a vested interest in the continued success of both. ■

REGION II



NJDOT Implements Real-Time Traffic Alert System for Commercial Vehicles

The New Jersey Department of Transportation (NJDOT) implemented a real-time traffic alert system for commercial motor vehicle drivers, making New Jersey one of the first states in the country to offer this safety feature.

The system offers in-cab traffic congestion updates and slowdown alerts to commercial motor vehicle drivers on 647 miles of New Jersey's highways, including the New Jersey Turnpike, Garden State Parkway and Atlantic City Expressway. Commercial motor vehicle drivers will be alerted about two to three miles before the slowdown begins, giving them plenty of time to reduce speed to help prevent crashes.

"The ability to alert commercial vehicle drivers to unexpected traffic conditions will improve safety for everyone driving on New Jersey's highways," said NJDOT Commissioner Diane Gutierrez-Scaccetti. "By warning drivers of congestion that is miles ahead, drivers of large commercial vehicles will have the extra time needed to safely slow down."

The system was developed in partnership with Intelligent Imaging Systems – delivered to drivers through its wholly-owned subsidiary, Drivewyze Inc., provider of connected truck services – along with INRIX, a transportation data and analytics company. The alerts are available to all carriers and drivers using the Drivewyze PreClear software.

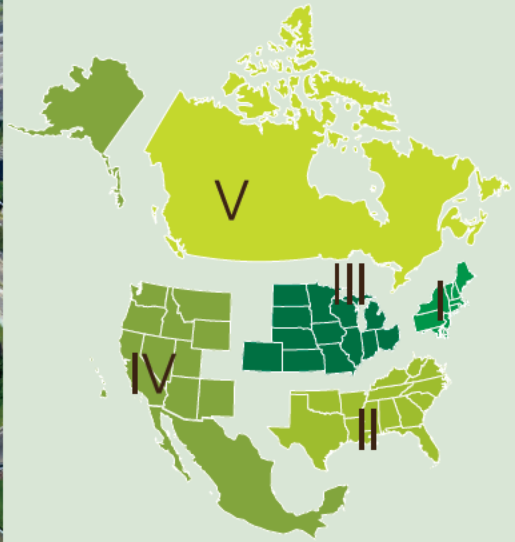
According to the trucking industry, a fully loaded tractor-trailer traveling at 65 mph takes 66% longer to stop than a passenger car. This can result in a collision if a truck does not have enough stopping distance. In the United States, nearly 30% of all collisions happen on interstates, with many being secondary crashes when a truck or car rear-ends a vehicle that was in a queue from an initial crash.

"The New Jersey Motor Truck Association applauds the efforts to provide advance safety alerts to commercial truck drivers via Drivewyze," said Gail Toth of the NJ Motor Truck Association. "These efforts will help to keep our workplace – the highways – safer for all."

The Drivewyze safety alert program is designed to help reduce commercial motor vehicle crashes and is a tool NJDOT has implemented as the state moves toward realizing its goal of zero deaths on its roadways.

The INRIX traffic and slowdown alerts will join other notifications that truck drivers already receive through Drivewyze's in-cab safety notification service, such as slowdown alerts when coming upon dangerous curves, and caution notifications when nearing a low bridge or mountain-corridor steep grades. The system will only send notifications to subscribed drivers within the geographical boundaries of New Jersey. Drivewyze is looking to offer similar geolocated services in other states.

Motorists are encouraged to check NJDOT's traffic information website, www.511nj.org, for construction updates and real-time travel information. For NJDOT news, follow the department on Twitter @NewJerseyDOT and Facebook. ■



REGIONAL MAP

Region I
Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Puerto Rico, Rhode Island, U.S. Virgin Islands and Vermont

Region II
Alabama, American Samoa, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia and West Virginia

Region III
Colorado, Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Northern Mariana Islands, Ohio, South Dakota and Wisconsin

Region IV
Alaska, Arizona, California, Guam, Hawaii, Idaho, Mexico, Montana, Nevada, New Mexico, Oregon, Utah, Washington and Wyoming

Region V
Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Northwest Territories, Nova Scotia, Nunavut, Ontario, Prince Edward Island, Quebec, Saskatchewan and Yukon

Oklahoma's Delaware County Implements Virtual Weigh Station

*By **Matt G. Ingham**, Point of Entry Program Administrator, Oklahoma Department of Transportation; and **Peter Fedechko**, Vice President, North America Sales, International Road Dynamics Inc.*

The Oklahoma Department of Transportation (ODOT) and Oklahoma Highway Patrol (OHP) have implemented the state's first virtual weigh station (VWS) for weighing and e-screening commercial motor vehicles entering from Arkansas via U.S. Route 412. The new VWS is located on the westbound lanes of the divided highway in Delaware County.

The goal of the project is to improve road safety by identifying potentially overweight vehicles and out-of-service vehicles and carriers through an expansion of the state's electronic screening network. The VWS allows OHP to monitor U.S. 412 the same way as more heavily traveled port of entry (POE) sites and will support targeted mobile enforcement, when needed. This will advance the mission of removing unsafe vehicles from the highway.

The VWS system technology and implementation was carried out by International Road Dynamics (IRD). The site design, installation and operation conform to the same project requirements as the Oklahoma POE e-screening sites deployed in recent years.

Commercial motor vehicles in both lanes are weighed by weigh-in-motion (WIM) scales to determine their compliance with weight restrictions for the vehicle's type and class. Vehicles are also checked by an over-height detection system.

The WIM sensors are IRD-PAT Bending Plate® scales installed in a double-threshold configuration for greater accuracy. Initial calibration indicated that the scales were measuring well within the American Society for Testing and Materials Type III standard for WIM accuracy. Lane 1 was measuring gross vehicle weight (GVW) with a maximum error of -2.4% in the test runs, while Lane 2 had only 0.9% maximum error in GVW during the test runs.

The two lanes are also equipped with automated license plate readers (ALPR) and U.S. Department of Transportation (USDOT) cameras for vehicle identification. All commercially classed vehicles have digital photos taken of their license plates and passenger-side doors so that the license plate and USDOT numbers may be extracted using optical character recognition (OCR) technology. The ALPR also determine the jurisdiction where the plate was issued. The OCR results are then screened against federal and state databases to identify the truck and carrier, and to screen against any related safety information.

The site uses IRD's iSINC® WIM controller to provide WIM screening and an IRD Intelligent Roadside Operation Credentialing (iROC) system to provide e-screening against SAFER and PRISM databases. The iROC obtains its credential and safety information from a centralized off-site server. A cell modem provides remote access to the site by authorized users.

All commercial motor vehicles traveling through the VWS are assigned a pass or fail status depending on e-screening settings and their compliance with weight regulations. Vehicles without credential identification are automatically assigned a fail status. When that happens, highway patrol can make a well-informed decision to pull the vehicle over for additional review.

Through a web-based interface, mobile enforcement personnel can also identify and select vehicles for weight enforcement or citations. Officers can pull flagged vehicles off the road to a designated area for weighing on portable weigh pads. The SAW III portable scales used are capable of dynamic (WIM) or static weighing. The static weights are National Type Evaluation Program-certified accurate so they may be used to issue citations. Static weights from the portable scales can also be entered into the VWS software to automatically calibrate the Bending Plate® scales to ensure they maintain optimal performance.

Additionally, the VWS software enables the state to collect high-quality commercial motor vehicle weight and screening data 24/7. The site will also be integrated with VI²M cloud-based central data reporting system in the near future to provide more options for data analysis. Additional daily reports will be sent to the Oklahoma centralized host operations computer. IRD's intelligent maintenance management service will provide a web-based interface for monitoring and reporting on maintenance service and equipment status.

The new Delaware County VWS advances the state's commercial motor vehicle enforcement program and will help OHP and ODOT improve road safety and infrastructure protection. Obtaining the same information through the same interface from both the virtual site and previously deployed inspection stations enables OHP to efficiently monitor operations across the road network. ■



A test truck crosses the WIM scales at the U.S. 412 VWS site.



iSINC® WIM Controller.



IRD-PAT Bending Plate® WIM Scales.

REGION II

Florida Highway Patrol Conducts Post-Crash Training Course

*By **Sgt. Denise Meredith**, Commercial Vehicle Enforcement, Training Unit, Florida Highway Patrol*

The Florida Highway Patrol (FHP) Commercial Vehicle Enforcement Training Unit conducted a post-crash training course in Orlando, Florida, Jan. 3-14. Students were instructed how to conduct a post-crash inspection following a traffic crash involving a commercial motor vehicle. Staff members from the National Training Center (NTC) attended a portion of the training to produce a training video for roadside inspections and safety investigators, at which time Capt. Bryant Gay demonstrated how an air braking system operates on a commercial motor vehicle. ■



Above from left to right: Darrin Frison, multimedia specialist, NTC; Ben Werner, curriculum manager, NTC; Sgt. Tim May, FHP; Capt. Bryant Gay, FHP; Tpr. Dave Morrison, FHP; Margie Rodriguez McQueen, safety programs manager, NTC; and Ian Keldin, videographer, NTC. **Below:** Capt. Bryant Gay, with the Florida Highway Patrol, demonstrates the air braking system operation on a commercial motor vehicle.





MARK YOUR CALENDAR

2022 ENFORCEMENT INITIATIVES

INTERNATIONAL ROADCHECK 2022

INTERNATIONAL ROADCHECK
May 17-19, 2022

OPERATION SAFE DRIVER

OPERATION SAFE DRIVER WEEK
July 10-16, 2022

Operation Airbrake

BRAKE SAFETY WEEK
August 21-27, 2022



North Carolina State Highway Patrol Commercial Vehicle Enforcement Updates

*By **Monica Y. Greiss**, Staff Development Specialist II, Commercial Vehicle Enforcement Section, North Carolina State Highway Patrol, North Carolina Department of Public Safety*

Safe DRIVE – Fifth Wave

The North Carolina State Highway Patrol participated in Operation DRIVE (Distracted, Reckless, Impaired, Visibility Enforcement) during the fifth wave of the program, conducted Nov. 22-24, 2021. Operation DRIVE is a high-visibility, multi-state traffic enforcement effort on interstate corridors spanning from North Carolina to Florida. This operation is designed to eliminate traffic fatalities by reducing crashes involving large trucks, buses and passenger vehicles, with the primary goal of changing unsafe driver behaviors.

For this operation, the North Carolina State Highway Patrol partnered with the South Carolina State Transport Police, Georgia Department of Public Safety's Motor Carrier Compliance Division, Alabama Highway Patrol, Arkansas State Police, Kentucky State Police, Tennessee Highway Patrol, Virginia State Police and the Florida Highway Patrol. The North Carolina State Highway Patrol conducted 1,885 commercial motor vehicle inspections, identified 168 out-of-service vehicles and placed 90 drivers out of service. Collectively, participating states conducted 4,949 commercial motor vehicle inspections. Inspectors placed 400 drivers and 680 vehicles out of service during the fifth wave of Operation DRIVE.

CVE Seatbelt Initiative

Troop B District 9 of the Commercial Vehicle Enforcement Section conducted a seatbelt initiative the week of Sept. 27, 2021. Officers conducted 260 inspections, consisting of 37 Level I Inspections, 81 Level II Inspections and 142 Level III Inspections. Thirty-four citations were issued, specifically for seatbelt compliance violations. ■









UPDATES FROM Mexico

SCT Becomes SICT

As of Oct. 21, 2021, as stated in the Official Gazette of the Federation, the Secretariat of Communications and Transportation (SCT) has changed its name to Secretariat of Infrastructure, Communications and Transportation (SICT). The Mexican Congress approved the change of name.

The functions and offices that currently belong to the Secretariat will not undergo any change. Likewise, relationships with other institutions, both national and international, will continue to function without any modification.

The change is one more advance in the constant work of this Secretariat, which continues with its commitment to provide citizens with better and safer roads as well as technological advancements of instruments and equipment for road safety.

President of the Republic Appoints New Undersecretary of Transportation in the SICT

As of Jan. 11, Carlos Alfonso Morán Moguel left his position as SICT undersecretary of transportation to serve as general director of Benito Juárez International Airport in Mexico City. Architect Rogelio Jiménez Pons, who has extensive experience in the transportation sector in Mexico, assumed the undersecretary of transportation position.



Pictured left to right: New Undersecretary Rogelio Jiménez Pons, Secretary Jorge Arganis Díaz Leal and Former Undersecretary Carlos Alfonso Morán Moguel.

Official Standard on Signaling and Road Devices for Streets and Highways Posted for Public Consultation

For its conference in January, the SICT and the Secretariat of Agrarian, Territorial and Urban Development – through the National Consultative Committee for the Standardization of Land Transport in conjunction with the National Consultative Committee for the Standardization of Land Use and Urban Development – published the proposed Official Mexican Standard PROY-NOM-034-SCT2/SEDATU-2021 in the Official Gazette of the Federation.

This project focuses on signaling and road devices for streets and roads, as a mechanism to lay the foundations for the formation of a harmonized signaling system in the national territory.

Continued on next page



Continued from page 7

It is a mandatory regulation, applicable throughout the national territory that will allow, among other benefits, the standardization of horizontal and vertical signaling as well as different road devices, contributing to road safety.

One of the main objectives of the NOM (its acronym in Spanish) is to give priority to road safety in the streets and highways of the country, following the narrative of the mobility pyramid, which places people as a priority.

A 60-day public comment time follows the publication of this new technical regulation. During this time, any person in the national territory may submit comments and identify areas of opportunity.

It should be noted that the NOM project, once approved as a definitive NOM, will replace the current horizontal and vertical marking of highways and urban thoroughfares established by NOM-034-SCT2-2011. The current NOM project broadens its scope in urban areas, provides greater emphasis on vulnerable users and incorporates signals and devices for mainly urban use.

For more information on the NOM project, visit www.dof.gob.mx/nota_detalle.php?codigo=5640134&fecha=04/01/2022. ■









Montana Travel Team Saturates Locations and Focuses on Level I Inspections

*By **Sgt. Matt Caudill**, Motor Carrier Services Enforcement Bureau, Montana Department of Transportation*

While the idea of a team organized to focus on high-risk areas in a jurisdiction isn't new to law enforcement, Montana's Travel Team is a new organization within our agency. This team is staffed by highly motivated officers from around the state and conducts a high number of inspections in areas that are not typically worked and show high traffic.

The Travel Team spends one week every month or every other month focusing on Level I Inspections. As can be imagined by those that work the road, a high quantity of inspections generally yields compelling results. Violations range from intoxicated drivers to significant mechanical violations as can be seen in the photographs. Over the course of 2021, the Travel Team conducted about 800 Level I Inspections, 114 Level II Inspections and 30 Level III Inspections. Of these inspections, 182 vehicles were placed out of service.

As with anything in Montana, the weather was the biggest adversary faced by the Travel Team, with highs over 100 degrees and lows in the single digits. They also contended with high winds and snow at various points in the year; however, they persevered and continued to put up excellent numbers, regardless of the elements. For all of these reasons, every member of Montana's Travel Team deserves recognition for fulfilling the mission of Montana Motor Carrier Services and protecting the traveling public from commercial motor vehicles operating under dangerous conditions. ■











DRUG RECOGNITION EVALUATION POST-INCIDENT REVIEW:

SOMETHING TO CONSIDER IN CASES WITHOUT AN EVALUATION

*By **Beth Barnes**, Traffic Safety Resource Prosecutor, Arizona Governor's Office of Highway Safety and the Arizona DUI Abatement Council, and Assistant City Prosecutor, City of Phoenix Prosecutor's Office*

Ideally, in any drug-impaired driving case, a complete drug recognition evaluation (DRE) is conducted during the initial investigation. Too often, however, a DRE is not called or is not available and no evaluation is performed. The absence of a contemporaneous DRE evaluation does not always mean the expertise of an experienced DRE officer cannot be beneficial. A DRE post-incident review (often referred to as a DRE reconstruction) may be worth considering.

DRE post-incident reviews are not new. Officers started conducting them in the 1990s. Yet, they have become a hot topic of late. Accordingly, the International Association of Chiefs of Police Technical Advisory Panel recently formed a working group that is preparing a list of considerations for those contemplating pursuing a post-incident review.

This group defined a DRE post-incident review as "a process utilized by certified drug recognition experts to provide follow-up investigative steps to collect, review, analyze, and interpret evidence and facts post-incident to render articulable facts and information, which may include opinions related to impairment." In other words, a post-incident review is the use of a qualified, experienced drug recognition expert to conduct an after-the-fact investigation to determine if there is enough information available to develop an expert opinion. The drug recognition expert then reports those findings and often testifies to them in court as an expert witness.

A DRE conducted on the date of violation is always superior to, and much more likely to be admitted into evidence, than a DRE post-incident review. One should never fail to call a drug recognition expert on the date of violation on the assumption that a DRE post-incident review can be conducted later.

Whether to pursue a DRE post-incident review should be carefully considered and undertaken with caution. DRE post-incident reviews are not for every case – or even most cases – where a DRE was not conducted at the time of violation. While they are a very useful tool, post-incident DREs should only be used under ideal circumstances, especially if they are new to a prosecutor's jurisdiction; do not risk creating bad law.

Below are some suggestions for deciding whether a DRE post-incident review is appropriate for a given case and tips for executing one.

Selecting a Drug Recognition Expert

Because the state will have to qualify the drug recognition expert, thought should go into determining who will conduct the DRE post-incident review and testify as a witness. When these reviews are performed, be sure to use a drug recognition expert with the extensive training and experience necessary to qualify him/her in court as an expert to conduct a DRE post-incident review.

To increase the likelihood the testimony will be admitted at trial, it is recommended that prosecutors use currently certified, long-serving DRE instructors who have conducted a large number of DREs. Their expertise and experience are much broader than just attending DRE school. These credentials better

Continued on next page

Continued from page 9

lend themselves to DRE post-incident reviews. Prior experience testifying as an expert is also beneficial.

Evaluating the Case

DRE post-incident reviews should not be casually embarked upon. The importance of scrupulously assessing the case to determine if it is appropriate for a DRE post-incident review cannot be overstressed. The likelihood that the review will be admitted in court should also be evaluated. A prosecutor should review his/her case to ensure there is sufficient information to allow the drug recognition expert to reliably form a supportable opinion. It is much easier to admit this type of testimony if toxicology results are available. In fact, trial courts often refuse to allow this type of testimony when toxicology results are lacking. If there are no toxicology results, there must be other, independent evidence of drug use, such as drugs, drug paraphernalia, admissions or witness statements.

If the drug recognition expert determines there is insufficient evidence for a supportable opinion, other parties must respect this decision. Avoid pressuring the drug recognition expert to do a post-incident review if he/she is not comfortable doing one. Do not pressure him or her to form an opinion. The drug recognition expert should not provide an opinion if there is not enough evidence to solidly support it.

Collecting Evidence

A common mistake made by parties new to DRE post-incident reviews is to rely only on the police report, toxicology results and other evidence from the initial investigation. The prosecutor and drug recognition expert also need to collaborate to collect as much additional evidence as possible to allow for a comprehensive review.

Just as in the case of traditional DREs, the drug recognition expert should interview the investigating officers and other witnesses. Not only does this provide the drug recognition expert with more information, but it is also one of the standard steps of the DRE protocol and, accordingly, something the trial judge may want. A review of trial and appellate court rulings suggests that the more closely the DRE post-incident review resembles a typical DRE evaluation, the more likely it will be admitted during trial.

Customary additional sources of data to be obtained by the drug recognition expert or provided by the prosecutor include:

- Police reports
- EMT or paramedic observations and reports
- Doctor and nurse observations and records
- Medical records and test results
- Body-worn recordings of officer contact with the suspect
- 911 or dispatch recordings
- Civilian witness observations
- Relevant video recordings
- The suspect's statements
- Circumstantial evidence found on or near the suspect, such as paraphernalia
- Crash reports
- Jail booking information
- Toxicology reports

This list is by no means all inclusive. Much thought needs to be put into what relevant evidence might be available, and the drug recognition expert should be prepared to testify to all the evidence that he/she reviewed.

Prosecutors must comply with local discovery rules and decide if the drug recognition expert needs to complete a supplemental report. Reports, opinions and testimony should include an account of the relied-upon evidence as well as any limitations. They should also clearly state that the opinions are based upon a post-incident review, not the drug recognition expert's drug influence evaluation or personal observation of the defendant.

Court Preparation and Testimony

The limits of testimony and form of expressed opinions should be carefully thought out by the drug recognition expert and prosecutor to ensure consistency with local legal constraints. Testimony can impact the fact finder as well as the future admissibility of this type of evidence across the country. The drug recognition expert should be cautious about rendering an opinion that the defendant was actually impaired or under the influence of a drug category. Testimony that the defendant exhibited symptoms of impairment consistent with drug use of a category or consistent with the reported toxicology results is a safer option and much more likely to be admitted.

The prosecutor will have to lay sufficient foundation in court to qualify the drug recognition expert as an expert for DRE post-incident reviews. This foundational showing should address more than the usual training and experience testimony and be specifically tailored to the DRE post-incident review issue. Much of the training and experience obtained by drug recognition experts, and especially instructors, lends itself quite well to this issue. Be sure to point out during testimony how the drug recognition expert's training and experience help prepare for DRE post-incident reviews.

Examples of areas to explore include:

- The fact that incomplete DREs are included in the DRE curriculum and in appropriate circumstances allowed by the protocol
- Cases in which the drug recognition expert was not able to complete the entire protocol process but was still able to form an opinion
- The fact that during training, drug recognition expert students watch videos of DREs they did not conduct and review face sheets they did not prepare, from which they must then describe impairment and form opinions
- Experience serving as a scribe
- Drug-impaired driving cases where a DRE was not conducted but the drug recognition expert was able to form a relevant opinion

- Previous DRE post-incident reviews
- Any training received for DRE post-incident reviews
- All relevant experience or training that would assist with a DRE post-incident review, including training as an EMT, crash reconstruction training, etc.

If the witness is a drug recognition expert instructor or state coordinator, he or she should have experience reviewing DRE reports conducted by others to ensure the correct call was made based on the evidence presented. This experience is particularly helpful in DRE post-incident reviews.

Additionally, the prosecutor and drug recognition expert should prepare for testimony, putting thought into how to:

- Explain the expert's ability to give an opinion even though he/she did not conduct an evaluation on the date of violation.
- Discuss the general indicators of impairment observed by the witnesses and how those observations relate to driving. If there is documented evidence of indicators, such as the person's blood pressure or pupil size, discuss how that evidence is relevant to the analysis.
- Tie toxicology results, drugs, paraphernalia and witness admissions to the symptoms of impairment exhibited on the date of violation and demonstrate how these are relevant. If the drug recognition expert knew the toxicology results before forming the opinion, prepare for the defense argument that the expert merely relied on the toxicology results to form the opinion.

A prosecutor should create a good record and consider providing the court with a pleading that incorporates case law from his/her jurisdiction and others where DRE post-incident reviews have been admitted. Make sure the testimony provided by the expert is detailed and thorough and that the prosecutor establishes an adequate foundation for the case being made.

The drug recognition expert should avoid testifying that a person was impaired by certain drugs or categories of drugs based solely on the post-incident review, behavioral observations or a quantitative toxicology result. Instead, it is preferable to explain that the observed signs and symptoms are consistent with use of the various drug categories or impairment. This type of opinion should generally be limited to cases where toxicology results support the presence of a certain category. Polycategory drug use must also be taken into consideration.

It appears from a review of transcripts and case law that most courts only allow the drug recognition expert to testify that the signs and symptoms of impairment the defendant exhibited on the date of the incident are consistent with the drugs that were in the blood or urine sample, or something similar. Rarely is the drug recognition expert allowed to give an opinion regarding the defendant's ability to safely operate a motor vehicle.

If this testimony is new to a prosecutor's jurisdiction or if there is concern regarding the court's willingness to admit this type of testimony, a prosecutor may want to begin by using DRE post-incident review as rebuttal evidence rather than in the state's case-in-chief.

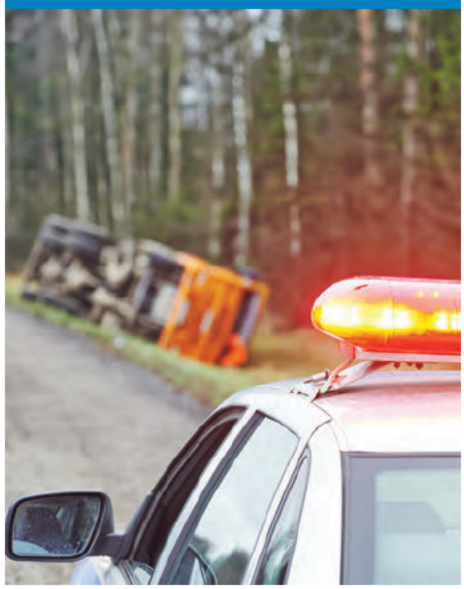
Case Law

The use of DRE post-incident review, or otherwise calling a drug recognition expert who did not participate in the investigation on the date of violation, has not been widely litigated. Published opinions allowing this type of testimony include Wooten v. State, 267 S.W.3d 289 (TX App.-Houston 2008); State v. Wynne, 182 CT App. 706 (App. 2018); People v. Ciborowski, 55 N.E.3d 259 (IL App. 2016); and State v. Neal, 267 NC App. 442 (2019). This type of testimony has also been used in a few additional states.

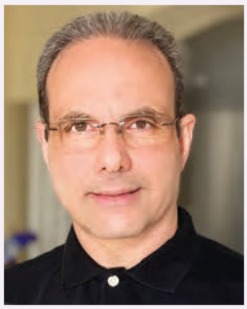
Conclusion

A DRE conducted at the time of the incident will always be preferable to a DRE post-incident review. The post-incident review should never be considered a replacement for the traditional DRE. However, if appropriately used, a DRE post-incident review can be an effective tool to strengthen a case where a contemporaneous DRE was not conducted. ■

The term "DRE post-incident review" has been recommended by the International Association of Chiefs of Police Technical Advisory Panel DRE Review Working Group in place of "DRE reconstruction" to avoid the potential of implying the standards used to admit crash reconstruction evidence should be applied to DRE post-incident reviews.



CVSA Welcomes Three New Staff Members



Rodolfo Giacoman joined CVSA in November 2021 as the fatigue management program specialist. He has collaborated with CVSA since 1993 as a contractor, associate member and sponsor. Most recently, Rodolfo served as general manager of Alertness.Pro for seven years, where he conducted education and training programs for motor carriers and commercial motor vehicle drivers on fatigue management, including the North American Fatigue Management Program. Rodolfo is a veteran program manager of mission-critical public safety programs and systems under federal and international contracts. During his two decades as a contractor for the U.S. Department of Transportation, Rodolfo developed his expertise in driver crash risk mitigation, enforcement information systems and international safety operations. He also performed periodic commercial motor vehicle inspections and maintenance for his family's trucking business. His first paying job was as a CDL driver of an articulated tow truck in intra-city and interstate operations. Rodolfo may be reached at rodolfog@cvsa.org or 301-830-6155.



Katie Morton joined CVSA in December 2021 as the hazardous materials specialist. She served 15 years with the Missouri Department of Transportation as an investigator, lead staff trainer and hazardous materials specialist, also acting as a subject matter expert on electronic logging devices and the 2020 hours-of-service rule changes. Additionally, she was a certified inspector who conducted safety audits, compliance reviews and complaint investigations. Katie has a Bachelor of Science degree in criminal justice and a master's degree in public affairs. She may be reached at katiem@cvsa.org or 301-960-1141.



Ariel Carter joined CVSA in January 2022 as the grants management specialist. She has years of experience administrating complex grant portfolios. Before joining CVSA, Ariel's professional background included designing, implementing and managing domestic and international grant programs as she worked as an intermediary on behalf of Fortune 500 companies, in addition to working with private foundations. Ariel has a Bachelor of Arts in criminology, Bachelor of Science in marketing and a master's degree in development studies. She may be reached at arielc@cvsa.org or 301-960-1142. ■

CVSA Offers Hazardous Materials Instructor Training

*By **Bill Reese**, Director of Hazardous Materials Programs, Commercial Vehicle Safety Alliance*

In fiscal 2021, CVSA received a Hazardous Materials Instructor Training (HMIT) grant from the Pipeline and Hazardous Materials Safety Administration. The purpose of this grant program is to provide training for hazardous materials (hazmat) instructors who train hazmat employees. That was the first time CVSA applied for that grant, which focuses on training the hazmat industry. The resulting training opportunity is open to anyone in the regulated hazmat community.

Last year, CVSA was able to hold four 40-hour HMIT courses, thanks to this grant. One in-person course was held in Salt Lake City, Utah, in September 2021. Due to the pandemic, three of the courses were held virtually. The 40-hour virtual courses were delivered in two different ways: either as five 8-hour days in one week or six shorter days over two weeks. We will continue to offer both formats for future virtual courses.

With either format, two days of the course are spent on team projects. Each team is given a hazmat training topic and required to develop a presentation on the assigned topic that involves all team members. Teams deliver their presentations to the rest of the course participants and are evaluated by the instructors and other participants.

Through this process, one of the things we've identified is the need for a more basic introductory course to hazmat instructor training. To address this issue, we are developing a 24-hour course that will address HMIT at a more basic level. The first course is tentatively scheduled for April.

Virtual and in-person training courses are scheduled throughout 2022. Visit www.cvsa.org/training for a list of training courses and dates.

You may also access an HMIT course and an archive of hazmat-specific webinars on CVSA Learning. **Visit www.cvsa.org/memberportal to log in. Click on the CVSA Learning tab, then select "Hazmat."** ■



Five Reasons Why Fatigue Is a Tough Cookie to Crack



*By **Rodolfo Giacoman**, Fatigue Management Program Specialist, Commercial Vehicle Safety Alliance*

Late last year, CVSA adopted a program that has little to do with enforcement and yet a lot to do with road safety: the North American Fatigue Management Program (NAFMP). NAFMP resulted from collaborative efforts by federal, state and provincial governments, along with industry organizations. It was developed by sleep and fatigue management scientists and field-tested by motor carriers from both Canada and the U.S., over the course of four development phases spanning more than a decade. Uniquely, it is sponsored by federal regulatory agencies but is entirely voluntary.

While the NAFMP seeks to reduce driver fatigue, it does not place the entire burden of fatigue management on drivers. It also considers the role played by drivers' families, motor carrier executives, managers, trainers, dispatchers, shippers, receivers and brokers. While it is a free program, it does require an investment to implement its five major components:

1. Safety culture
2. Fatigue risk management system
3. Sleep disorder screening and treatment program
4. Trip scheduling practices and fatigue management technologies
5. Education and training via a Train the Trainer Course with PowerPoint slides or the eLearning platform, both of which are available at nafmp.org (while on the NAFMP website, check out the return-on-investment calculator)

Some may wonder, why all the fuss? Aren't hours-of-service (HOS) rules and a good night's sleep all you need to avoid fatigue? Please consider the following five reasons why fatigue is a tough cookie to crack without a comprehensive strategy to address this multifaceted issue.

REASON 1

Fatigue Cannot Be Regulated

HOS rules allow drivers to sleep and rest, and compliance with these rules is proven to lower crash rates. They are generally enforceable and encourage periods of rest to combat fatigue.

However, HOS rules are not a proactive approach, less a comprehensive one. In addition to the time on the job, several

Continued on next page



Continued from page 13

factors contribute to driver alertness (see more on these factors under Reason 4). It is impossible to regulate all fatigue risk factors or what drivers do in their free time. Being on a break does not necessarily mean a driver is resting. For these reasons, a proactive and comprehensive approach to address, optimize and manage all fatigue risk factors is needed in addition to HOS regulations.

REASON 2

Fatigue Is Hard to Measure

Accounting for fatigue-related crashes is difficult because fatigue can contribute to crashes in subtle ways. Drivers may not recognize that their responses were dulled by exhaustion or admit to falling asleep at the wheel. Drivers may not even recall what happened before the crash. Tragically, drivers may also be severely injured or killed in the crash, leaving few clues as to the cause. Also, it can be difficult to distinguish between fatigue, distraction and other crash factors.

However, we know what a typical fatigue-related crash looks like. It is usually a single-vehicle road departure crash occurring between 2-7 a.m. These crashes mostly happen when the driver is alone and often on monotonous roads. The worst part is that fatigue-related crashes are usually serious, resulting in injuries or death.

In a 1990 study, the National Transportation Safety Board (NTSB) estimated that fatigue was the principal factor in 31% of crashes resulting in a driver fatality. This 32-year-old study has long been considered the best estimate on fatigue-related crashes. More recently, the AAA Foundation for Traffic Safety found that the occurrence of crashes involving drowsiness is nearly eight times higher than federal estimates show, based on in-vehicle dashcam video research analysis. The AAA report stated that "the difficulty of detecting drowsiness following a crash makes drowsy driving one of the most underreported traffic safety issues."

To combat this risk, motor carriers need to establish a fatigue risk management system to monitor and deter fatigue-related incidents using fatigue management technologies as recommended by the NAFMP.

REASON 3

Fatigue Is Difficult to Identify

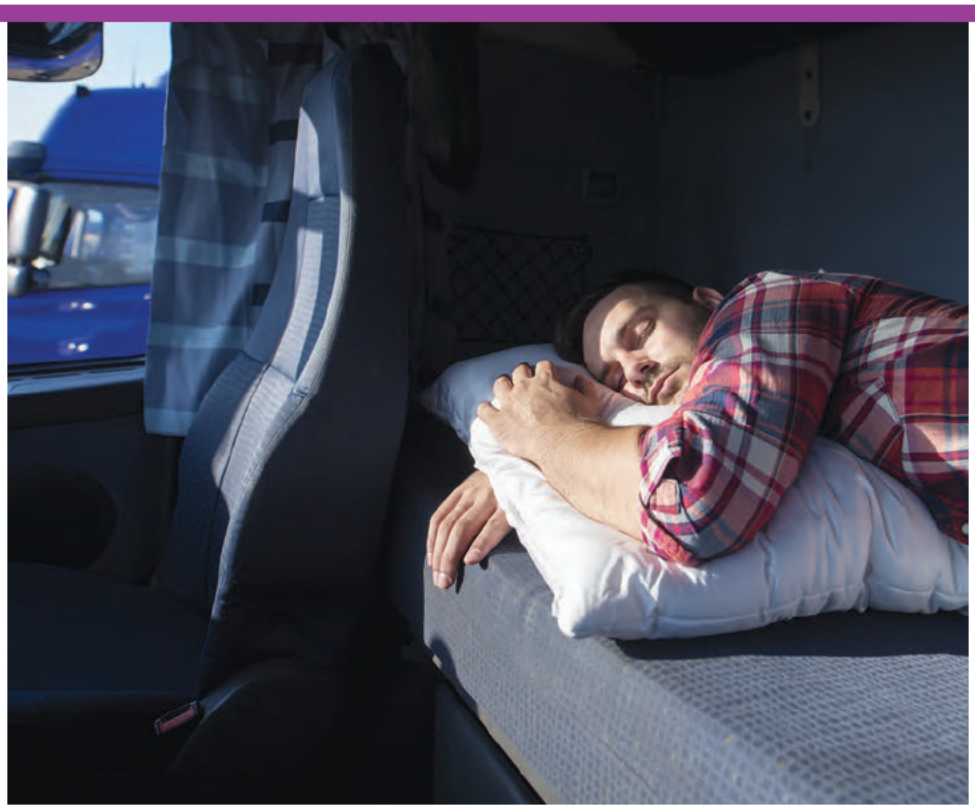
Realizing that we are fatigued is not always easy. Our self-assessment bias makes us believe that we are safe drivers even when we are not at full capacity. A driver fatigue and alertness study found that drivers overestimate their alertness. Self-ratings were often inaccurate compared to objective measures of alertness. Self-ratings tend to be based on expectations rather than reality, such as "I just started driving, so I couldn't be tired." Additionally, most driving is a solitary activity, so we cannot directly compare our performance to that of others.

That's why the NAFMP includes driver training to identify objective signs of fatigue. Among others, these signs include eyelid drop, yawning, wandering thoughts, swaying or jerking head movements, reduced field-of-vision, fidgeting, adjusting the HVAC, crossing the rumble strip, drift and jerk steering, delayed or incorrect responses and, the worst, microsleeps.

REASON 4

Fatigue Has Supply and Demand Factors

Two general categories of factors affect alertness: supply and demand. Supply factors are also called internal factors. They include the amount and quality of sleep, time of day (which influences one's biological clock, aka circadian rhythm), time awake (which affects the biological stopwatch, aka sleep pressure or homeostatic sleep drive), use of stimulants or other drugs, overall health, genetic predispositions and mood. These supply/internal factors are what determine our individual fatigue susceptibility in any given moment. Having a good night's sleep is not that simple if you have the scheduling, job demands and sleeping conditions of a



» Still, the gold standard countermeasure is taking a break with a nap.

commercial driver; more so if you have a sleep disorder or chronic condition that increases fatigue, such as fibromyalgia.

That's why the NAFMP provides drivers with education on how sleep works and its effect on the supply factors. That's also why a sleep disorder screening and treatment program is one of the five critical components of a fatigue management program.

On the demand factors side, there are two subtypes – task factors and environmental factors. Task factors include time on task, task complexity and task monotony. Tasks that are too complex or too monotonous increase fatigue; the ideal is a "Goldilocks task," where the balance between complexity and monotony is just right. Environmental factors include road conditions, weather, heat, noise, vibration, vehicle design, light conditions, social interaction (increases alertness but may be distracting) and other stimulation.

So even if a driver has supply or internal factors covered, including getting a good night's sleep, the demand factors can still reduce alertness and cause fatigue-related crashes.

The NAFMP provides drivers with training on several countermeasures against fatigue regardless of the type of factors affecting their alertness. Still, the gold standard countermeasure is taking a break with a nap.

REASON 5

Alertness is a Spectrum, Not a Switch

Alertness does not act like an on-and-off switch. We do not go from being fully awake to asleep or vice versa instantly. It is more like a spectrum. Think of it like a fuel tank indicator. In the full position, we are fully alert. In the empty position, we are asleep.

Fatigue management comes into play for what happens between fully alert and asleep. At three-quarters of a tank, we are less alert but still able to function. At the halfway mark we are in a state of reduced vigilance (aka hypovigilance). This is when we develop a reduced field of view or tunnel vision (aka highway hypnosis, white line fever and sleeping with your eyes open). Micronaps, drifting off for 30 seconds or less, sometimes without the driver realizing, occur at the quarter-full mark, when we become drowsy.

In this alertness vis-à-vis fuel-tank analogy, the big difference is that a vehicle will function perfectly fine until the indicator hits empty. Alertness, on the contrary, requires a full or an almost full alertness tank to function correctly.

How do you keep your drivers operating with a full alertness tank? Implement the five components of the NAFMP as mentioned earlier. If you are a driver, take advantage of the fatigue management education and training provided in module 3 of the NAFMP to learn more about the problem of fatigue, the science of sleep, how to objectively identify fatigue, what you can do to manage it, fatigue myths and practical dos and don'ts of fatigue management. And that – working together to employ comprehensive fatigue-reduction strategies that support our commercial motor vehicle drivers – is the way the driver fatigue cookie crumbles. ■

New NAFMP Resources

- **Webinars open to the public**: Go to nafmp.org/webinars to register for upcoming live webinars or watch previous recordings.
- **eLearning Forum:** When enrolling for free at lms.nafmp.org in any of the NAFMP courses, please join the conversation or ask questions in the fatigue management forum by navigating to the site home from the left-side menu.

CVSA's 2022 Out-of-Service Criteria Available for Purchase

CVSA offers different formats of the new out-of-service criteria. Find the format that works best for you.

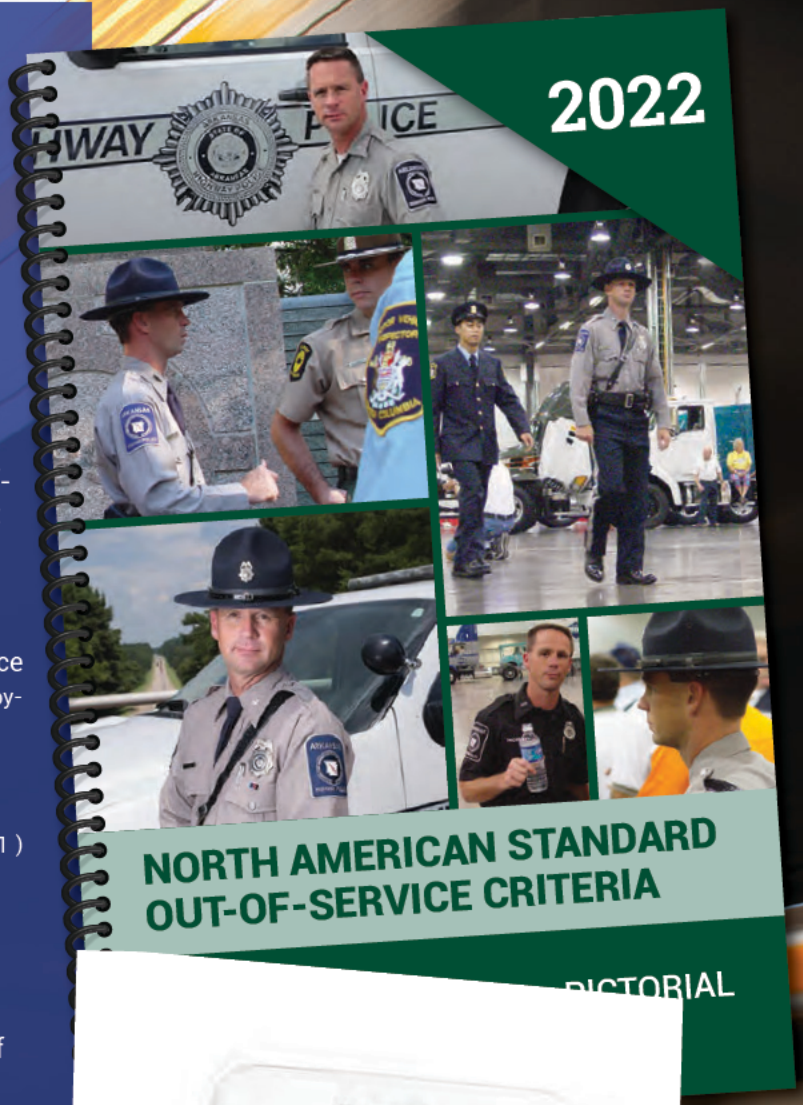
- Spiral-bound, hard-copy handbook
- Electronic PDF file with a restricted three device and/or web browser limit (cannot be pr nted or copy-and-pasted and s best v ewed on a desktop computer)
- Spanish U.S. version (8 5 x 11)
- Bilingual English/Spanish U.S. version (8 5 x 11)
- French Canadian version (8 5 x 11)
- Bilingual English/French Canadian version (8 5 x 11)

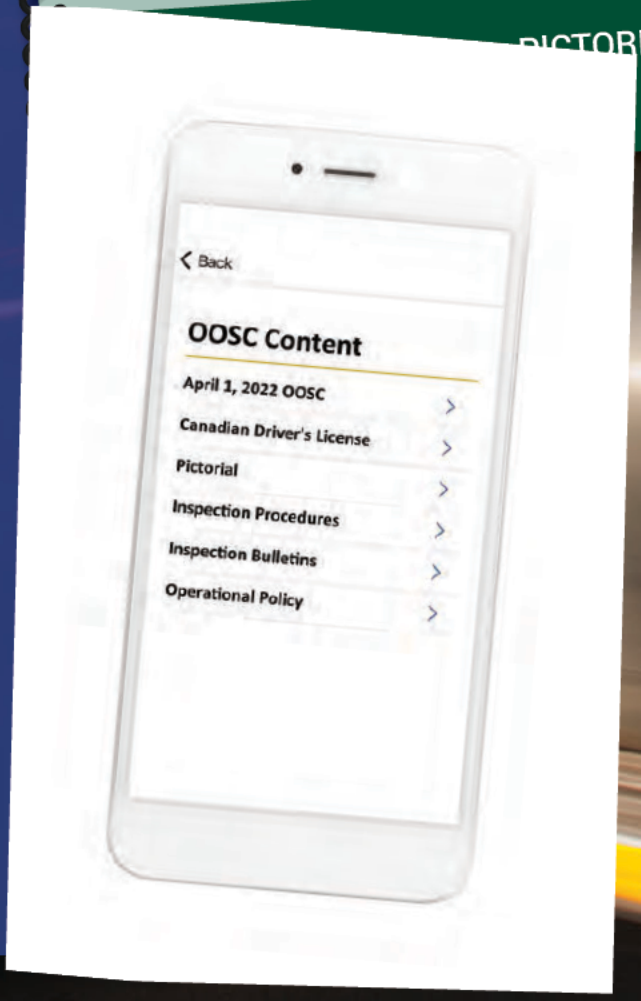
To purchase one of the above-listed versions of the out-of-service criteria, visit www.cvsa.org/store.

If the app is more your style, it contains the out-of-service criteria, inspection bulletins, real-life photo examples of vehicle, cargo securement and hazardous materials/dangerous goods violations, access to the CVSA Learning portal for online training, inspection procedures, operational policies, inspection and educational videos, brochures, and more.

To download the app, search for "CVSA" in the Apple Store or Google Play. Select "CVSA Out-of-Service Criteria." Once you've downloaded the app, set up your account with your first and last name and email address. You'll then have the option to purchase the 2022 out-of-service criteria.

CVSA







INSPECTOR'S CORNER

Competition

*By **Sgt. Benjamin Schropfer**, Nebraska State Patrol; 2019 North American Inspectors Championship Grand Champion*

It's been a long wait, but we are finally getting close. If anyone out there is still reading these articles, you are probably thinking, "Yes, this guy has been doing this for too long. It is time for someone new." However, my extended reign as North American Inspectors Grand Champion is only part of what I'm talking about.

As you read this, we are getting closer to CVSA's North American Inspectors Championship (NAIC) and the American Trucking Associations' National Truck Driving Championships (NTDC) and National Step Van Driving Championships, which were last held in person during August 2019 in Pittsburgh, Pennsylvania. The events are scheduled to return this August in Indianapolis, Indiana. So, we can all collectively hold our breath and knock on wood with the hope that nothing happens, or has already happened before this is published, to disrupt those plans.

By the time this article comes out, it may be too late for some of you to compete this year, as some states and companies have already chosen their competitors. If that is the case, there is always next year. Many of you, both inspectors and drivers, may have never considered throwing your hat in the ring for these championships. Others may have tried but may not have made it to the big show. Whatever the case may be, I encourage you to challenge yourself to enter the fray when the opportunity arises.

There are a wide variety of ways for you to be selected to participate in these events. Drivers need to compete in and win their state's competition to qualify for the national competition. Some of you may also need to compete in your company's own version of the competition to move forward to your state competition. The process varies for us inspectors as well. Many jurisdictions have their own competition in order to select who will represent them at NAIC, while others use a different selection process. Although many companies and jurisdictions have already made their selections, others are gearing up for state competitions as you read this. If you still have the opportunity to participate, I encourage you to take advantage of it.

These competitions are a great occasion to recognize the work we do each day. I cannot speak for the driving championships, but as an inspector, there are always a lot of spectators there to cheer on the competitors. The awards ceremony is pretty amazing, too.

I can also say that NAIC is very family friendly. That is one of the things I've enjoyed most – the chance for my wife and family to see what I do and watch my success be recognized. Of course, I also enjoy the competition itself and the chance to test myself against some of the best inspectors in North America. So, if you are fortunate enough to represent your organization at NAIC or the NTDC, I would encourage you to take your family with you.

Earlier, I said to challenge yourself. When NAIC first began in 1993, it was referred to as "Challenge," and I think that's appropriate. Just trying to make NAIC or any of the national driving competitions requires challenging yourself. Then, if you do make it to the big competition, a whole new level of challenge awaits. While the staff and facilitators are there to challenge you, grade you and rank you among your peers, it all comes down to you challenging yourself.

Even when there's no championship title on the line, you should challenge yourself at everything you do each day. Every day, every inspection, every trip, every action — do it the best you can. Others can present you with a challenge, but it's how you react that truly matters. Do you take every opportunity to improve yourself, your skills and your knowledge? Or do you accept "good enough" and just get by? It may be a cliché, but I believe that if you are not getting better, you are probably getting worse.

Notice that I say challenge yourself to do the best you can. I would go even further and say this: do the best you can at that time. You can't always be the very best and win every competition or challenge presented to you. Sometimes, there is just someone better than you are – or better on that particular day.

I was fortunate enough to win NAIC in 2019. Now, I'm not trying to be too modest. I acknowledge that it took a lot of hard work to get myself there. However, I'm also not saying that means I'm the best ever. Any one of my fellow competitors that year had the ability to win that competition and every year there are new and worthy competitors. There had been 26 champions before my win. Any one of those champions or any of the champions yet to come may have beaten me if they had been there in 2019. In fact, many of them had beaten me in prior competitions. Even some of the competitors I faced in Pittsburgh may have won on a different day or under different circumstances.

I was very fortunate to be given the opportunity to represent Nebraska in more than one NAIC, going a total of five times. Each time, I had to first win our state competition, and that in and of itself is something I am proud of. I had various levels of success in those earlier years at NAIC. I was proud of my accomplishments every time, but at the same time, I always had the nagging feeling that I could do better. I still had that feeling even in 2019. The difference was I just happened to have a better day than my fellow competitors that year.

That feeling that you can do better is what drives us. Not everyone is fortunate enough to have the opportunity to go to NAIC or the NTDC more than once (or to go even once, for that matter). Ultimately, it doesn't matter if it's NAIC, the NTDC or the inspection or trip you do every day – you should strive to do your best and challenge yourself to do even better the next time.

So, challenge yourself in everything you do and take the opportunity to compete either in NAIC or the NTDC. I guarantee you will not be disappointed. I hope to see you in Indianapolis. ■



Sgt. Schropfer's family attended and supported him at 2019 NAIC in Pittsburgh, Pennsylvania, where he won Grand Champion.



THE LEGISLATIVE AND REGULATORY RUNDOWN

States Face Opportunities and Challenges as They Tackle Safety Challenges on the Road

By **Adrienne Gildea**, *Deputy Executive Director, Commercial Vehicle Safety Alliance*

As this column highlighted in the previous edition of Guardian, last year, Congress and the Biden Administration came to an agreement on the Infrastructure Investment and Jobs Act, aka the Bipartisan Infrastructure Law. The legislation outlined a bold vision for national infrastructure investment over the next five years with a dramatic increase in funding for federal transportation programs, including those administered by the Federal Motor Carrier Safety Administration (FMCSA). That column also focused on the challenges jurisdictions will face in investing those new funds quickly and how best to have a measurable impact on combatting the alarming recent trends in roadway safety data.

Building on the historic investments included in the infrastructure bill and in response to the recent increase in crashes and roadway fatalities, in January the U.S. Department of Transportation launched its National Roadway Safety Strategy (NRSS) (see page 22 for more information). The NRSS represents a shift to the Safe System approach to transportation planning and marks the department's commitment to achieving the goal of zero roadway fatalities. The transportation safety community has a tremendous opportunity to capitalize on the current heightened attention on and commitment to roadway safety at the federal level.

With this renewed focus and the increase in federal funds, the states are faced with the expectation that they will implement policies and programs that will swiftly and effectively improve safety on our roadways, reducing the occurrence and severity of crashes. The jurisdictions stand ready to do just that, expanding existing solutions and exploring new ideas and opportunities. However, as the dust begins to settle and work gets underway, an old, familiar roadblock stands on the horizon – delayed access to and a lack of stability in federal funding.

As of press time, Congress had approved yet another continuing resolution for fiscal 2022 funding, this time through mid-March, extending programs and funding levels at the fiscal 2021 funding levels, which are well below what was envisioned for fiscal 2022 based on the passage of the bipartisan infrastructure bill. We will once again find ourselves midway through the year with no clear answer on when (or even if) the new approved funding levels will reach the jurisdictions.

CVSA has long written about, testified to and asked for assistance with the delays in getting federal funds out to the states each year. In order to maintain effective programs, states need to be able to plan long term. FMCSA cannot award funds until an appropriations bill is in place – a process that regularly sees delays well into the fiscal year. These delays leave states unsure of final funding levels, which makes it difficult to plan and structure a program. This is a challenge states have come to expect and around which program managers do their best to adjust.

However, this year, this longstanding problem is exacerbated by the tremendous discrepancy between the two possible funding levels. States are essentially being asked to develop and be prepared to implement two different sets of programs, depending on when or if the funds become available.

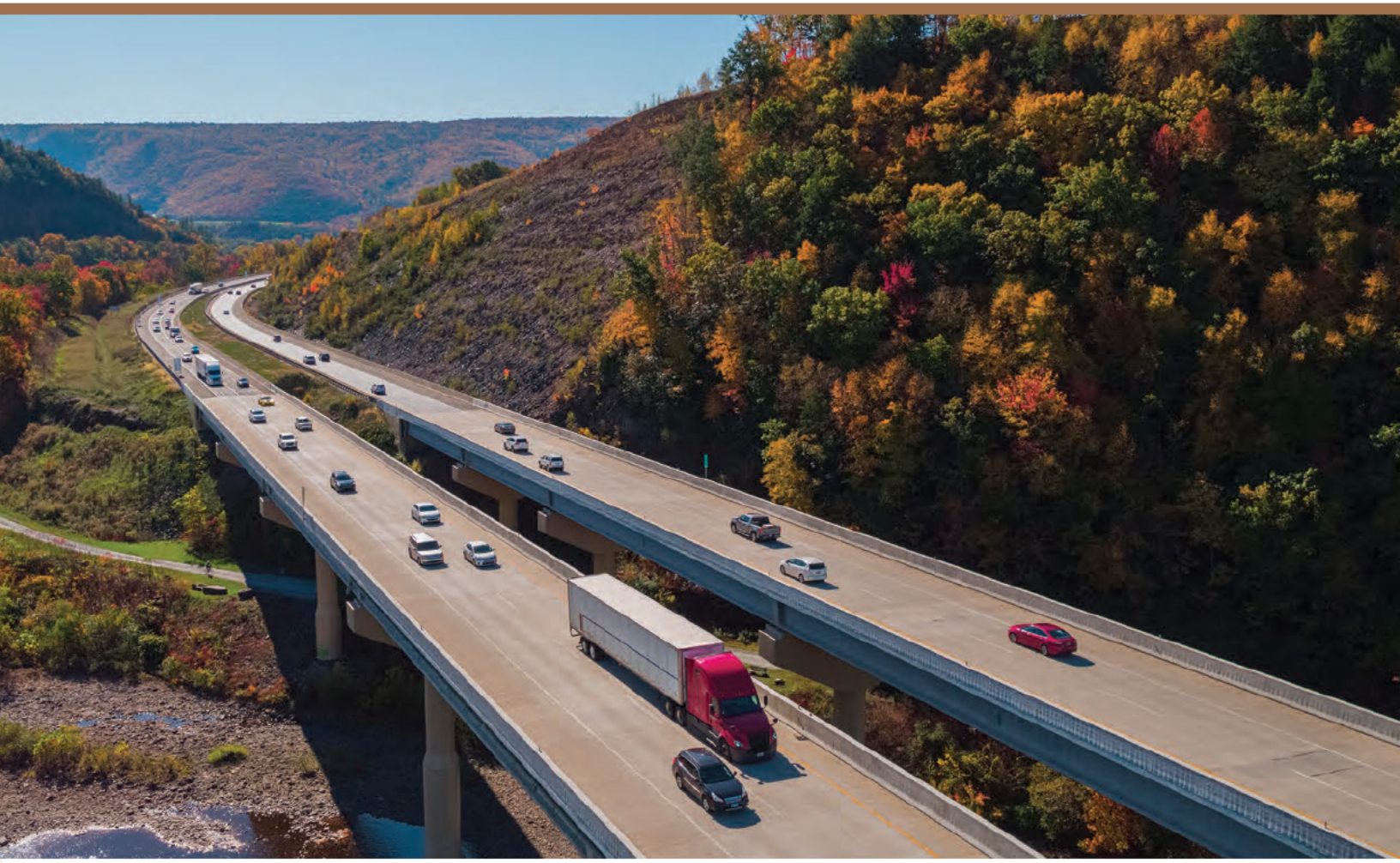
And the problem doesn't go away once the fiscal 2022 funding questions are answered. State program managers will have to decide how confident they are that the higher funding levels are sustainable beyond the current bill cycle. Will Congress maintain these high funding levels when the next appropriations bill is passed or will funding drop down to more moderate levels? How do the states set up programs that are agile enough to respond to any future funding changes?

This uncertainty will continue to limit the ability of jurisdictions to fully realize the potential for increased road safety offered by the infrastructure bill. As mentioned, this uncertainty has long been a challenge for the states. It has merely been made more prominent this year. It is imperative that Congress and others work to find a long-term solution that allows states to refocus their efforts on meeting program goals rather than on figuring out how to sustainably structure programs without secure funding.

Like the challenges outlined in the last edition of this column, this challenge of planning for unpredictable funding levels and timing is real, but not unsolvable. It's imperative that those with the ability to address this challenge work to find a way to provide states with more stability and continuity. The commercial motor vehicle safety community does not want to miss this opportunity to serve the shared mission of reducing crashes, injuries and fatalities on our roadways. ■



On Nov. 15, 2021, President Joe Biden signed into law a $1.2 trillion bipartisan infrastructure package.



U.S. DOT Provides More than $27 Billion to Fix Bridges Nationwide

Earlier this year, the U.S. Department of Transportation launched the historic Bridge Replacement, Rehabilitation, Preservation, Protection and Construction Program (Bridge Formula Program). The program, to be administered by the Federal Highway Administration (FHWA), represents the single largest dedicated bridge investment since the construction of the interstate highway system – providing $26.5 billion to states, the District of Columbia and Puerto Rico over five years and $825 million for tribal transportation facilities. The total amount available to states, D.C. and Puerto Rico in fiscal 2022 is $5.3 billion along with $165 million for tribes. The FHWA also published initial guidance on the new program.

"The Biden-Harris Administration is thrilled to launch this program to fix thousands of bridges across the country," said U.S. Transportation Secretary Pete Buttigieg. "Modernizing America's bridges will help improve safety, support economic growth, and make people's lives better in every part of the country – across rural, suburban, urban and tribal communities."

"This record amount of funding, made possible by the Bipartisan Infrastructure Law, will allow states and tribal governments to fix the bridges most in need of repair," Deputy Federal Highway Administrator Stephanie Pollack said. "It will also modernize bridges to withstand the effects of climate change and to make them safer for all users, including cyclists and pedestrians. Every state has bridges in poor condition and in need of repair, including bridges with weight restrictions that may force lengthy detours for travelers, school buses, first responders or trucks carrying freight."

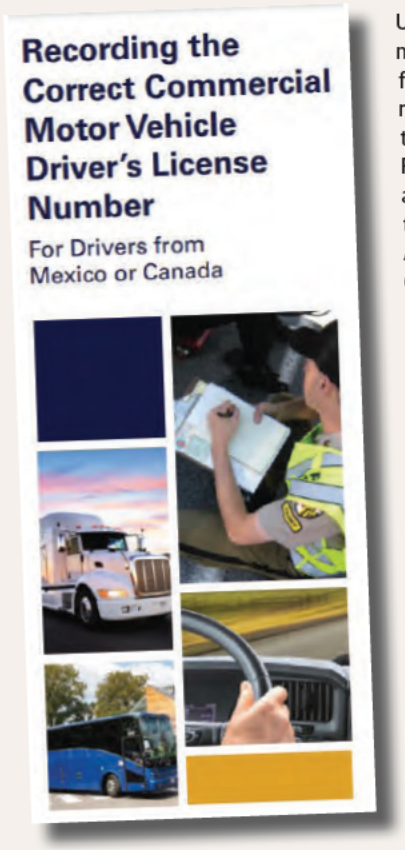
Nationwide, the Bridge Formula Program is expected to help repair approximately 15,000 highway bridges. In addition to providing funds to states to replace, rehabilitate, preserve, protect and construct highway bridges, the Bridge Formula Program has dedicated funding for tribal transportation facility bridges as well as "off-system" bridges, which are generally locally owned facilities not on the federal-aid highway system.

The Bipartisan Infrastructure Law includes an incentive for states to direct the new Bridge Formula Program funds to off-system bridges owned by a county, city, town or other local agency. While states generally must match federal funding with up to 20% state or local funding, the new guidance notes that federal funds can be used for 100% of the cost of repairing or rehabilitating such locally owned, off-system bridges.

The Bipartisan Infrastructure Law is a once-in-a-generation investment in infrastructure with the potential to grow the economy, enhance U.S. competitiveness in the world, create good jobs and make the U.S. transportation system more sustainable and equitable. Specific to the FHWA, the Bipartisan Infrastructure Law provides more than $350 billion over five fiscal years for surface transportation programs. ■

FMCSA Creates Brochure on Recording the Correct Driver's License Number for CMV Drivers From Mexico or Canada

*By **David Yessen**, Chief, Compliance Division, Federal Motor Carrier Safety Administration, U.S. Department of Transportation*



U.S. citations issued to commercial motor vehicle (CMV) drivers from Mexico or Canada that result in a conviction found in the Title 49 Code of Federal Regulations § 383.51 tables are added to the driver's history in the Federal Motor Carrier Safety Administration's (FMCSA) Federal Convictions and Withdrawal Database – but only if the correct license alphanumeric/character format is recorded.

These convictions can result in drivers being prohibited from operating in the U.S., making it critical to accurately record the driver's first and last name, date of birth, licensing jurisdiction and commercial driver's license number following the appropriate jurisdictional licensing scheme.

FMCSA has developed a new informational brochure to increase U.S. law enforcement personnel's awareness of the correct driver's license number configurations when writing citations for drivers from Canada and Mexico.

The trifold brochure, titled "Recording the Correct Commercial Motor Vehicle Driver's License Number for Drivers from Mexico or Canada," should improve the foreign license and conviction data reported to the Commercial Driver's License Information System and Federal Convictions and Withdrawal Database.

Download a printable version of the brochure from the FMCSA International Safety webpage at www.fmcsa.dot.gov/international-programs/recording-correct-commercial-motor-vehicle-drivers-license-number-drivers.

If your state enforcement office would prefer hard copies of the brochures, please reach out to your local FMCSA division office. ■

FMCSA Registration Overview

*By **Jeff Secrist**, Chief, Licensing and Insurance Division, Federal Motor Carrier Safety Administration, U.S. Department of Transportation*

As of November 2021, more than 730,000 interstate motor carriers have an active USDOT number and are registered with the Federal Motor Carrier Safety Administration (FMCSA) to operate on our nation's highways. These motor carriers play a critical role in transporting goods, services and our loved ones throughout our country's roadways and are vital to the nation's economy.

Approximately 650 new applicants register through FMCSA's online Unified Registration System each day. This reflects a 53% increase in new applicants from fiscal 2020 to 2021, with numbers continuing to rise in fiscal 2022.

By providing carriers with resources and information they need to register and safely begin operating — highlighted by a series of new and upcoming videos for applicants — FMCSA's Office of Registration hopes to make life easier for those navigating the registration process.

"Our goal is to make sure new carriers are prepared to operate – and operate safely – on the roads we all share," said Kenneth H. Riddle, director of FMCSA's Office of Registration. "By offering helpful, easy-to-use resources that provide clarity on the registration process and addressing common questions we get directly from carriers, we can move one step closer toward this goal."

The latest FMCSA resource available to applicants is an instructional video, "How to Register: FMCSA Registration Overview for Motor Carriers." It is available online at www.fmcsa.dot.gov/registration.

Released in September 2021, this video walks users through the registration process with clear, need-to-know information so they fully understand the necessary steps. It also refers carriers to additional resources to answer questions pertaining to their unique operations.

Producing this and other videos that respond to real-world feedback is a priority for the Office of Registration, contributing to FMCSA's commitment to reducing crashes, injuries and fatalities involving large trucks and buses. Two additional videos are in development, focused on entity types and operating authority, aiming to provide tailored guidance and address common questions FMCSA has heard from applicants.

"We pay close attention to what we hear from our new registrants," Riddle noted. "If we can prevent confusion and streamline the process, we can make it easier for carriers to participate in our shared safety mission."

The latest video has been viewed more than 16,500 times since its fall release. The Office of Registration has received positive feedback, with users noting they are looking forward to upcoming videos.

"We are delighted that the video is resonating with our audiences," said Riddle, adding, "Stay tuned for more." ■



U.S. Bureau of Transportation Statistics Announces a Vehicle Inventory and Use Survey

The U.S. Bureau of Transportation Statistics (BTS) announced the return of its vehicle inventory and use survey (VIUS) after nearly 20 years. The VIUS has been the principal data source on the physical and operational characteristics of the U.S. truck population. Its primary goal is to gain an understanding nationally and statewide of how trucks are being utilized for various goods transport. The 2021 VIUS is being conducted in partnership with the Federal Highway Administration, the Department of Energy and the U.S. Census Bureau to better understand the characteristics and use of vehicles on our nation's roads. The data will be used to guide investments in our nation's infrastructure and vehicle technologies and parts, and to evaluate truck safety needs, emissions estimates and conservation practices.

The 2021 VIUS will collect data from 150,000 vehicle owners of class 1 through 8 trucks, which includes pickups, SUVs, minivans, light vans, straight trucks and truck tractors. Dependent on what type of vehicle a selected driver owns, they will receive either the heavy-vehicle or light-vehicle questionnaire. The survey will be conducted through October 2022 and will collect information on the selected vehicle's 2021 activity, uses and physical characteristics. Vehicles from all sectors of the economy, households and states will be included. BTS plans to release the results in the fall of 2023.

The VIUS will collect data on:

- Vehicle safety technologies, such as collision warning, parking assist and vehicle-to-vehicle communications
- Vehicle fuel types, including alternative fuel sources
- Vehicle maintenance and level of repairs
- Uses of vehicles, including frequency of use, their capabilities, how far they travel and why they travel
- Miles traveled and fuel economy by weight, type, configuration and age of vehicle
- Axle configurations, trailers hauled and operating weight
- Equipment added after manufacture of the chassis
- Business versus personal use and types of economic activity served
- Commodities carried
- And much more

Current VIUS estimates are of critical importance to federal agencies, state departments of transportation, metropolitan planning organizations, businesses and drivers alike.

Results from the survey will:

Provide statistics for:

- Vehicle size and weight studies
- Tracking the deployment of driver-assistance technology
- Input to freight demand models and air quality models
- Role of motor vehicles in the economy
- Fuel efficiency of the nation's truck fleet
- Analyses of fees and allocation of cost among highway users
- Highway traveler exposure to potential safety risks

Guide investments into:

- Better roads, bridges, fueling stations and other transportation infrastructure at the local and state level
- Decreasing traffic congestion and energy usage on the nation's roadways
- Increasing safety and the ability to move goods more effectively ■

Milestones	Planned Completion
Survey Release	February 23, 2022
Survey Conclusion	October 2022
Data Release	Fall 2023



U.S. Department of Transportation Releases Comprehensive National Roadway Safety Strategy



In January, the U.S. Department of Transportation (DOT) released its new comprehensive National Roadway Safety Strategy (NRSS), a roadmap for addressing the national crisis in roadway fatalities and serious injuries. Almost 95% of the nation's transportation deaths occur on its streets, roads and highways. While the number of annual roadway fatalities declined for many years, progress plateaued over the last decade and now, alarmingly, fatalities have risen during the pandemic. The NRSS provides concrete steps that the department will take to address this crisis systemically and prevent these tragic and avoidable deaths and serious injuries. Bolstered by historic funding included in President Biden's Bipartisan Infrastructure Law, the NRSS is the first step in working toward an ambitious long-term goal of reaching zero roadway fatalities.

"We cannot tolerate the continuing crisis of roadway deaths in America. These deaths are preventable, and that's why we're launching the National Roadway Safety Strategy – a bold, comprehensive plan with significant new funding from President Biden's Bipartisan Infrastructure Law," said U.S. Transportation Secretary Pete Buttigieg. "We will work with every level of government and industry to deliver results, because every driver, passenger and pedestrian should be certain that they're going to arrive at their destination safely, every time."

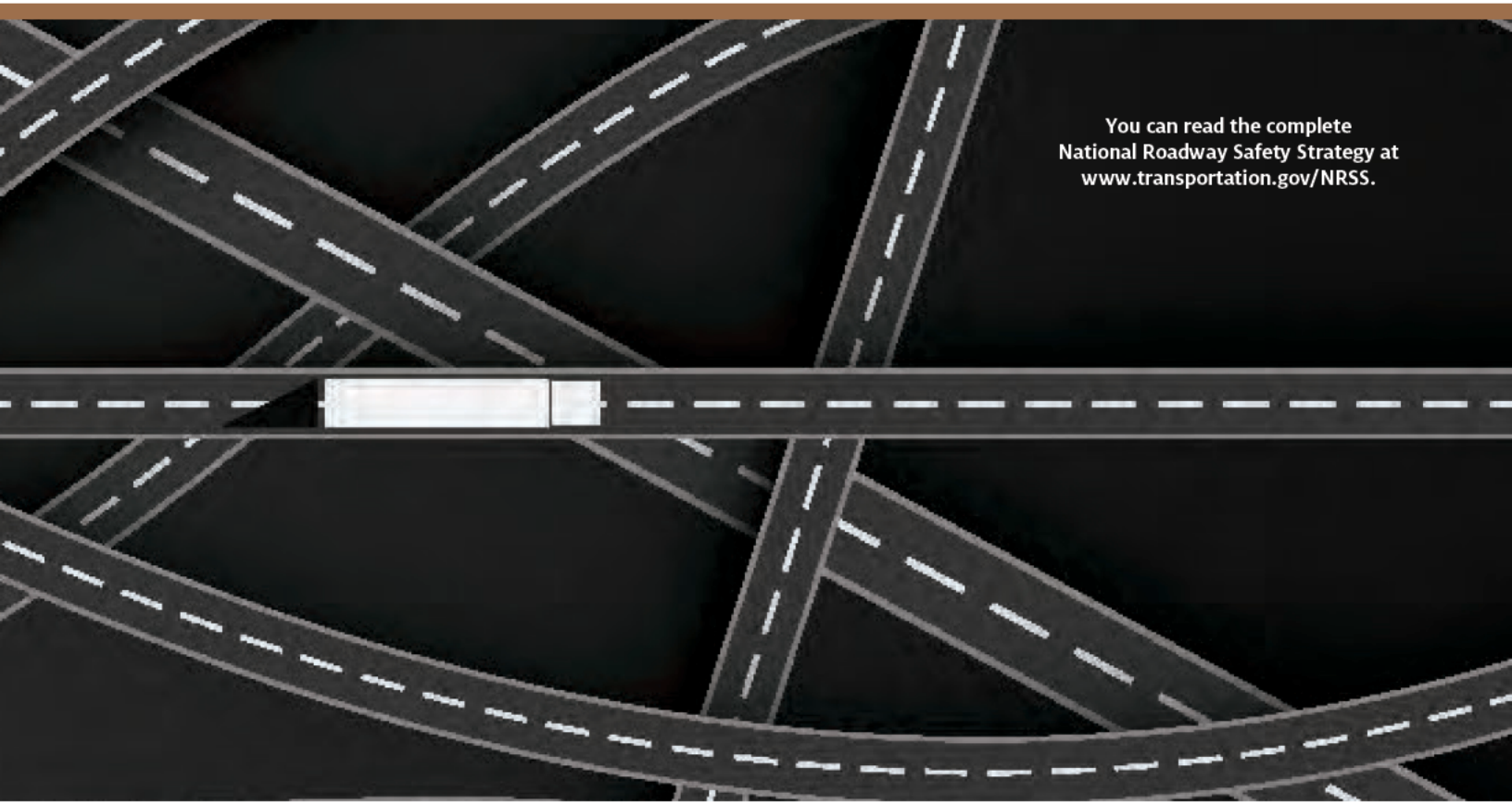
The department, as part of the NRSS, is adopting the Safe System Approach, which acknowledges human mistakes and vulnerability, and designs a redundant system to protect everyone by preventing crashes, while ensuring that if they do occur, they do not result in serious injury or death. The department will use a five-pronged model to address safety: safer people, safer roads, safer vehicles, safer speeds and post-crash care. Importantly, the NRSS also recognizes that reducing traffic fatalities will take sustained and concerted action from everyone across all sectors and levels of government.

The strategy was developed in coordination with the department's Executive Safety Council, led by Deputy Transportation Secretary Polly Trottenberg. The NRSS builds on and harmonizes efforts from across the department's three roadway safety agencies: the Federal Highway Administration (FHWA), the National Highway Traffic Safety Administration (NHTSA) and the Federal Motor Carrier Safety Administration (FMCSA).

"This National Roadway Safety Strategy represents a collective effort across the Department, and under the leadership of Secretary Buttigieg, to embrace the Safe System approach, and to recognize that no loss of life on our nation's roadways is acceptable. As we move towards swift implementation, we look forward to partnering with every level of government, industry, advocacy, and all who will come together to address this crisis," said Robin Hutcheson, former U.S. DOT deputy assistant secretary for safety policy, and acting administrator for FMCSA.

A few of the key action items in the NRSS include:

- Working with states and local road owners to build and maintain safer roadways through efforts including: updates to the Manual on Uniform Traffic Control Devices, a Complete Streets Initiative to provide technical assistance to communities of all sizes, and speed limit setting.



You can read the complete National Roadway Safety Strategy at www.transportation.gov/NRSS.

- Leveraging technology to improve the safety of motor vehicles on our roadways, including rulemaking on automatic emergency braking and pedestrian automatic emergency braking, and updates to the New Car Assessment Program.
- Investing in road safety through funding in the Bipartisan Infrastructure Law, including a new $6 billion Safe Streets and Roads for All program, hundreds of millions for behavioral research and interventions and $4 billion in additional funding for the Highway Safety Improvement Program.

Additionally, the NRSS recognizes that roadway safety is inextricably linked with the Biden-Harris Administration's equity and climate goals. Fatalities due to traffic crashes disproportionately affect communities of color, people living in rural areas, people with disabilities and older adults. Also, traffic deaths among people who walk or bike are increasing more sharply than for people who drive.

"Unfortunately, many roads are not designed to ensure safe travel at safe speeds for everyone, especially the most vulnerable road users," said FHWA Deputy Administrator Stephanie Pollack. "The Bipartisan Infrastructure Law provides a tremendous opportunity for FHWA to work closely with state, local and tribal partners to put increased transportation funding to work incorporating safety for all users into every federally-funded road project."

"FMCSA is committed to reducing commercial motor vehicle fatalities and overall fatalities. We will work across the department to coordinate proactive compliance and outreach programs and work collaboratively with all stakeholders," said FMCSA Executive Director and Chief Safety Officer Jack Van Steenburg. "Our goal is to prevent crashes and preserve the quality of life for all roadway users across America. Zero is our goal."

"No longer can we, as a society, accept traffic deaths as routine. Every life lost is a tragedy, and we all can, should, and must do more to change the culture. The National Roadway Safety Strategy and the Safe System Approach offer all communities a roadmap to save lives and reduce injuries," said NHTSA Deputy Administrator Dr. Steven Cliff.





Continued on page 25



CVSA OFFERS TRAINING THROUGH ITS ONLINE LEARNING PORTAL

CVSA's online learning management system, CVSA Learning, offers the flexibility for you to take a training course anytime, anywhere, at a speed that's comfortable for you.

Want to learn how to properly document a vehicle violation? We've got you. Do you know the properties of a Class 2 hazardous material? We'll teach you. Need some guidance on reporting and classifying motor vehicle crashes? There's a manual for that. Visit CVSA Learning to learn about these topics and much more.

Whether you're a law enforcement official, a motor carrier safety manager, a professional driver, a transportation safety advocate or an executive at a trucking organization, there is training in the CVSA Learning portal for you.

CVSA®

To access CVSA Learning, log into your CVSA member portal at www.cvsa.org/memberportal, then click on the "CVSA Learning" tab.

Continued from page 23

The Bipartisan Infrastructure Law provides new tools and resources that allow coordinated action both across the department and government. It also provides $6 billion for the Safe Streets and Roads for All program, $4 billion in additional funding for the Highway Safety Improvement Program and an additional infusion of $4 billion for improved crash data and vehicle, behavior, and truck safety programs. The FHWA will share updated guidance on the Highway Safety Improvement Program.

"The Roadway Safety Action Plan is designed to focus all of U.S. DOT's resources, authorities and incredible expertise, working with our stakeholders, to combat the tragic number of fatalities and serious injuries we see on U.S. roadways – from our largest cities and towns to rural and tribal communities all across the country," said Deputy Secretary Trottenberg.

The Bipartisan Infrastructure Law, also known as the Investment in Infrastructure and Jobs Act, is the Biden-Harris Administration's plan for building a better America with a $1.2 trillion investment in the nation's infrastructure and economic competitiveness.

The Bipartisan Infrastructure Law will rebuild America's roads, bridges and rails, upgrade and expand public transit, modernize the nation's ports and airports, improve safety, tackle the climate crisis, advance environmental justice and invest in communities that have too often been left behind. It will also drive the creation of jobs and grow the economy sustainably and equitably so that everyone gets ahead for decades to come. ■



SAFER VEHICLES

CVSA Supports the U.S. DOT's National Roadway Safety Strategy

Some of the priorities identified in the NRSS specific to the commercial motor vehicle enforcement and motor carrier industry communities include:

- Implementation of the October 2021 final rule that requires state driver's licensing agencies to access and use information obtained through the Drug and Alcohol Clearinghouse and take licensing actions against commercial motor vehicle drivers who have drug or alcohol violations in the system and are not cleared to return to duty
- Improved accuracy of commercial driver's license (CDL) driver records and the identification of additional opportunities to use these more accurate records to take unsafe commercial motor vehicle drivers off the road more expeditiously
- Increased highly visible commercial motor vehicle traffic enforcement targeting risky driving behaviors, especially speeding – the department identified speed enforcement, deployed equitably and applied appropriately to roads with the greatest risk of harm due to speeding, as a tactic that may provide significant safety benefits and save lives
- Continued commitment to identifying high-risk companies and operators of commercial motor vehicles using a data-driven and performance-based approach, including roadside commercial motor vehicle safety inspections

"As we embark on this reinvigorated effort, we are relying on our partners to also identify and commit to near-term actions that will help make our collective efforts to reach zero a reality," said Transportation Secretary Buttigieg.

CVSA's membership is committed to supporting the U.S. DOT in its commitment to zero fatalities on our roadways through the implementation of identified safety priorities and the Safe System approach.

"On behalf of the Alliance, I'd like to thank Transportation Secretary Buttigieg and the U.S. Department of Transportation for their leadership and action in this undertaking," said CVSA Executive Director Collin Mooney. "We look forward to working together toward our shared vision of zero roadway deaths." ■



While the Country Slowed Down, Drivers Sped Up: *What This Means for Teens*

*By **Stacey Tisdale**, CPPE, PMP, Project Manager, Youth Transportation Safety Program, Texas A&M Transportation Institute*

Youth continue to be overrepresented in car crashes throughout the United States. According to data from the National Highway Traffic Safety Administration (NHTSA) and the Centers for Disease Control and Prevention (CDC), motor vehicle crashes continue to be one of the leading causes of injury and death for people under the age of 25 in the U.S., with young drivers having much higher crash rates than older, more experienced drivers.

In June 2021, NHTSA estimated crash fatalities for the 16 to 24 age group increased by 15% in 2020, challenging notable progress over the previous few years when we'd seen a downward trend. More recent NHTSA reporting, for early 2021, gives an even more disturbing early estimate of overall crash fatalities of 18.4% . They went on to attribute this overall increase to use of drugs and alcohol, lower uses of seat belts and riskier behavior, including extreme speeding (defined as 20 miles per hour or higher over the posted speed limit).

We at the Texas A&M Transportation Institute Teens in the Driver Seat (TDS) program wonder how young drivers have and will fare for the current time period and beyond. As we wait for all 2020 data and 2021 estimates to be released and hope for a decline in these numbers in 2022, the risks mentioned above have not subsided even though roadway travel has almost met pre-pandemic levels.

In a time when many of us may feel a lack of control, we know these are trends we can change. The first year of licensure is the most dangerous time for new drivers and bad habits can begin to show up during the first few months of driving on their own. For teens that have just begun driving during these past two years, we wonder if they are adopting these risks they see mirrored by many other drivers currently, such as speeding, low seatbelt use and impairment.

Additionally, while for many years these behaviors have been identified as top driving risks for teens, they are outranked by distractions and nighttime driving. The idea that teens have completely stopped distractions and possibly adopted one of these other risky behaviors instead is far-fetched, so we may assume that they are accumulating a combination of risky habits which will place them at even greater crash risk.

Many teens, and even their parents/guardians, are unaware of the risks they face behind the wheel. Some of the most recent findings from knowledge surveys administered to TDS program schools (11,314 surveys from July 2019 to July 2021) demonstrated only 27% and 32% of teens identified talking on a cellphone and using social media as common risk factors for teen drivers, and only 9% identified driving at night.

The TDS program looks to teens to change trends of crashes through positive peer influence since we know that teens learn from each other and influence behaviors of their



⚠ NHTSA attributes overall increase of crash fatalities to use of drugs and alcohol, lower uses of seat belts and riskier behavior, including extreme speeding (defined as 20 miles per hour or higher over the posted speed limit).

peers. We provide the research, materials and incentives for teen teams to conduct evidence-based outreach and activities in their school and community so their influence can include traffic safety.

The Federal Motor Carrier Safety Administration supports these efforts to keep all road users safe by providing funding for additional resources and education for driving safely around large trucks and buses and provides support for the You in the Driver Seat app, which rewards young drivers with gift cards for driving distraction-free and within speed limits – all behaviors that are national best practices and have been shown to work.

There are also other mitigating factors that work, including adult influence. Just as teens influence each other, seasoned drivers can demonstrate safe driving so teens develop better habits in this impressionable time. Whether you have a teen getting ready to enter the learning phase of driving or a young adult with a license, there are a number of ways to help them stay safe:

- Be the driver you want your teen to be. Young children begin watching you drive well before they ever get behind the wheel.
- When driving with your teen in the car, talk through what you are doing and why, such as checking the mirrors, steps to changing lanes or looking both ways before accelerating at a green light.
- Make sure everyone in your family abides by zero tolerance for cell phone use while driving. If you know your teen is driving, don't call them.
- Know that each passenger, including siblings, in a teen's car increases the likelihood of a crash.
- Don't push a teen who, for whatever reason, is not ready to drive safely.
- Allow your teen as much driving practice as possible (at least 50 hours), with you present.
- The first year of licensing is most dangerous. Continue to check in with your teen by riding with them to look for any new bad habits.
- Shared family vehicles are safer for young drivers than having their own.
- Involved parents have safer teen drivers. Talk through each driving trip before your teen leaves – gauge their state-of-mind, know where they are going, how they will get there and their timeline. If your teen is stressed, tired, upset or even too excited, they shouldn't drive.
- Use your state's Graduated Driver Licensing (GDL) laws as only a baseline for rules. Many state GDL laws do not go far enough to protect young drivers.

It's difficult to add one more way this pandemic has negatively changed the world around us, but there is good news. Car crashes are preventable. They're controllable. We can't say that about a lot right now. ■

How the National Transportation Safety Board "Most Wanted List" Can Make Our Roads Safer

*By **Nicholas Worrell**, Chief, Safety Advocacy, National Transportation Safety Board*

Last year, the National Transportation Safety Board (NTSB) issued its Most Wanted List (MWL) of Transportation Safety Improvements. The list sets the board's advocacy priorities for a two-year period and is designed to increase awareness of, and support for, the most critical changes needed to reduce transportation accidents and to save lives. It features 10 safety-critical focus areas. For this advocacy cycle, half of the priorities focus on critical improvements needed for highway safety.

Why does our list focus so much on highway improvements? Although the NTSB investigates accidents in all modes of transportation, without a doubt highway safety is our biggest concern – and advocacy challenge.

In 2020, as our nation struggled with the challenges of a worldwide pandemic, we also faced an ongoing and increasing public health crisis on our roads. While vehicle miles traveled were historically low, the country still saw a dramatic increase in traffic crashes, fatalities and injuries. Nearly 40,000 people died on our nation's roads and millions more were injured that year. Unfortunately, early data indicates that another dramatic increase in roadway fatalities occurred in 2021. The National Highway Traffic Safety Administration (NHTSA) estimates that 20,160 people died in motor vehicle crashes during the first half of 2021 – an 18% increase over the same period in 2020.

Both NHTSA and the Federal Motor Carrier Administration (FMCSA) pointed to speeding as a significant issue in crashes involving trucks and passenger vehicles – a focus area for CVSA in 2021 during Operation Safe Driver Week. Other crash factors of concern included:

- Distraction
- Occupant ejection (up 20%)
- Unrestrained occupants of passenger vehicles (up 15%)
- Speeding (up 11%)
- Police-reported alcohol involvement (up 9%)

The NTSB's 2021-2022 Most Wanted List focuses on addressing many of these crash causes – in particular, speeding, impairment, distraction, vulnerable road users, and collision-avoidance and connected-vehicle technologies.

For instance, "Implement a Comprehensive Strategy to Eliminate Speeding-Related Crashes" is on the list. In deciding to include it, we noticed that between 2009 and 2018, speeding-related crashes resulted in nearly 100,000 fatalities – that's close to one-third of all traffic fatalities in the United States. The true extent of the problem is likely underestimated because the reporting of speeding-related crashes is inconsistent. To address this pressing safety concern, we must make full use of all the tools and strategies at our disposal. Speed limiters on large trucks, automated enforcement, expert speed analysis tools and education campaigns remain underused.

The NTSB has called for a paradigm shift in how we address road safety. We believe in and strongly advocate for the adoption of the Safe System Approach, a key part of our advocacy in 2020 and an item on our current MWL. In September 2020, NTSB Chair Jennifer Homendy urged government and law enforcement officers – the entire highway community – to embrace this approach when tackling road safety.

The principles underpinning the Safe System Approach acknowledge that humans make mistakes that lead to traffic crashes, but no one should lose their life or be seriously injured because of a crash. The Safe System Approach also recognizes that:

- The human body has a limited physical ability to tolerate crash forces
- Road safety is a shared responsibility
- All parts of the system must be strengthened so that if one part fails, road users are still protected

NTSB has held several roundtables with experts on the Safe System Approach, which may be viewed on our YouTube page.

The NTSB cannot improve highway safety alone. We need every voice and authority on the ground. Highway safety advocates, government organizations and law enforcement officers have a big task ahead. After all, effective road safety advocacy requires three parts: legislation, education and enforcement.

Addressing the causes of fatal accidents and reversing the emerging crash trends will be a challenge, but we know that we are not alone in this fight; together we can and will make a difference. ■

2021-2022 NTSB MOST WANTED LIST

NTSB's 2021-2022 Most Wanted List highlights transportation safety improvements needed to prevent accidents, reduce injuries and save lives. NTSB urges lawmakers, industry, advocacy and community organizations, and every American to learn more about what they can do to implement and champion the 2021-2022 Most Wanted List recommendations.

The list has four categories: aviation, highway, marine and rail, pipeline and hazardous materials. The highway recommendations are:

- Implement a comprehensive strategy to eliminate speeding-related crashes.
- Protect vulnerable road users through a Safe System approach.
- Prevent alcohol- and other drug-impaired driving.
- Require collision-avoidance and connected-vehicle technologies on all vehicles.
- Eliminate distracted driving.

View NTSB's Most Wanted List at www.ntsb.gov/mwl.





What to Do If You Suspect a Staged Accident

*By **Jim Angel**, Vice President of Video Telematics, EROAD*

"In-cab video for commercial vehicles is the single best tool to protect a commercial operator and a commercial driver from insurance fraud on the highways."

Research shows that commercial drivers are at fault for serious truck-car accidents far less often than passenger car drivers. Still, large accident-related verdicts against motor carriers – many exceeding $1 million – have become increasingly frequent in recent years, according to the American Transportation Research Institute's (ATRI) 2020 report, *Understanding the Impact of Nuclear Verdicts in the Trucking Industry*.

The trend toward larger verdicts against carriers has attracted the attention of criminal groups that target commercial trucks with staged-accident schemes, an issue that was brought to the forefront last year when the federal indictments of dozens of people charged with participating in staged accidents in Louisiana made headlines.

Staged accidents can be devastating to individual carriers. But the impact of staged-accident fraud and the general trend toward larger verdicts are also felt industry-wide in the form of skyrocketing insurance rates.

The ATRI report referenced above, for instance, cites one motor carrier that was forced to cease operations in 2019 after its insurance premiums more than doubled year over year. "Multiple other fleets, many decades-old family businesses, experienced similar outcomes," ATRI concluded.

Given the far-reaching impact of staged accidents on the trucking industry, it's crucial that motor carriers take steps to protect their businesses and the industry overall. The first step is for carriers and drivers to get educated on common staged accident scenarios and indicators.

Common staged accident scenarios include:

- **Swoop and squat:** One perpetrator vehicle cuts off the victim and slams on the brakes after a second vehicle has pulled up alongside the victim, blocking them in and preventing them from swerving to avoid the collision.
- **Start and stop:** The fraudster slams on their brakes in front of the victim, causing a crash. This scenario may play out during stop-and-go traffic.
- **Sideswipe:** A perpetrator vehicle swerves into the victim and claims that the victim crossed over into their lane. This staged crash may occur at busy intersections with dual left-turn lanes.

Other indicators that an accident might be staged include:

- **Multiple passengers:** Staged accident perpetrators want to maximize the profits, and that means cramming as many people into the car as possible to increase the number of fraudulent injury claims.
- **Jump-ins:** Sometimes "passengers" may enter a vehicle after the collision and later claim that they were injured in the accident. So-called "jump-ins" are a huge red flag for fraud.
- **Pre-existing damage:** Perpetrators often use beat-up cars for staged accidents. Look for vehicle damage that is not consistent with the crash.
- **Vehicle condition:** Look for things like heavy dust and dirt on the vehicle, weathered tires, and old windshield wipers. These are all signs that the car isn't regularly used and was only brought out for the staged accident.

If a staged accident is suspected, it's crucial that drivers immediately share any relevant information with responding law enforcement and their safety supervisor to ensure that fraud is considered during the accident investigation.

Matthew J. Smith of the Coalition Against Insurance Fraud, who participated with EROAD in a webinar series on staged accidents, suggests that commercial drivers also use a smartphone to photograph the aftermath of an accident – the position of the vehicles on the road, the conditions of the vehicles, the debris field – and provide that information to responding officers.

Smith also suggested a technology solution that can help protect carriers against fraud: video-based onboard safety management systems.

"In-cab video for commercial vehicles is the single best tool to protect a commercial operator and a commercial driver from insurance fraud on the highways," he said. ■

How Carriers Can Lead with Lagging Indicators

*By **Dave Elniski**, Industry Advisor, Alberta Motor Transport Association*

In the field of occupational health and safety (OHS), indicators of a workplace's performance can be broadly divided into two categories: lagging indicators and leading indicators. Lagging indicators are measurements of incidents that have occurred in the past, whereas leading indicators are predictive of future OHS incidents.

Organizations are usually most familiar with lagging OHS indicators, such as injury rates and incident reports in the workplace. For a motor carrier's highway safety program, examples of lagging indicators include collision rates, incident reports and violations/fines from law enforcement.

While leading indicators can be more complicated to use than lagging indicators, they are valuable measurements for proactive motor carriers. Examples of workplace leading indicators include number of workplace inspections performed and worker training rates. For a carrier's on-highway safety performance, leading indicator examples could be pre-trip frequency and quality, hours-of-service (HOS) performance and ongoing driver training activities.

Generally speaking, using lagging indicators is reactive while using leading indicators is proactive. However, proactive and reactive are connotation-loaded words, with many considering proactive safety superior to reactive safety. It is true that being proactive can prevent a loss (such as from a collision), whereas reactive safety management typically kicks in once a loss (be it an accident or fine) has occurred. However, all indicators are valuable to a carrier; even a highly proactive company can experience a loss. When that happens, it should go into reactive mode, investigating and implementing any warranted corrective actions.

Focusing only on one type of indicator while neglecting the other isn't the best approach. Carriers should develop a system for monitoring both lagging and leading indicators, use all available information to improve safety and stay abreast of best practices to improve proactivity, along with creating processes for reacting to any incidents.

On-road law enforcement provides carriers with an external inspection system into the workplace, driver behavior and carrier safety practices. Any negative feedback from law enforcement is a lagging indicator. Examples include fines for unsafe driving, out-of-service declarations for violations of CVSA's North American Standard Out-of-Service Criteria and noted defects on an inspection report.

In this way, on-road law enforcement is a generator of lagging indicators for carriers, flagging existing problems in a manner that results in a loss for the carrier and driver.

While it's best to prevent a violation-laden inspection report or fine, once a carrier receives one, it is time to be strategically reactive. First, carriers must work to meet any reporting requirements for the cited defects and pay or dispute any incurred fines. Second, the carrier should implement its internal processes for correcting the problems that led to the violation. These corrective actions may include driver discipline, driver or technician training and internal evaluation. Remember, being reactive is not intrinsically bad; reacting and responding are the only options once a carrier learns of a negative incident.

Still, being reactive does come at a cost. There is a benefit to becoming more proactive by learning from lagging indicators, which typically have a corresponding leading indicator that could influence future rates of the respective lagging indicator. Here are some examples:

Lagging indicator: A driver was placed out of service for an HOS violation.

Corresponding leading indicator: The carrier's internal HOS monitoring frequency, depth and follow-up.

Lagging indicator: A roadside inspection report identified rubbing air lines and a drum brake pushrod measuring over its brake adjustment limit.

Corresponding leading indicator: The carrier's frequency of routine vehicle inspections and maintenance for those components.

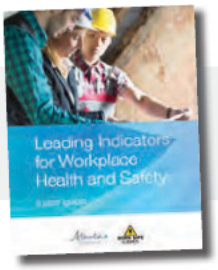
Lagging indicator: A carrier was ticketed for being overweight on an axle group.

Corresponding leading indicator: The frequency and depth-of-knowledge by which drivers are trained in legal weights and loading procedures.

Carriers are capable of monitoring and measuring each of the above leading indicator examples. The key takeaway is this: examples of past poor performance provide opportunities for systematically improved future performance.

By identifying and paying attention to leading indicators, a carrier will see a decrease in the corresponding lagging indicators, reducing the risk of a future negative event. For example, a carrier can monitor HOS records and proactively notify drivers of issues, preventing drivers from receiving HOS-related violations from law enforcement, as well as reducing the risk posed by driving without rest. In this way, carriers can take more control of their future safety performance.

When carriers understand, track and value both leading and lagging indicators, they can learn from a bad day and discover a pathway to better, safer days ahead. ■



Reference: Government of Alberta. 2015. "Leading Indicators for Workplace Health and Safety: a user guide." Accessed Jan. 7, 2022, from https://open.alberta.ca/publications/9781460120941.

Training, Research and Education for Driving Safety Program Offers Train the Trainer Workshops to Increase Driving Safety Awareness and Decrease Distracting Driving Behaviors Among Commercial Drivers

*By **Jill Rybar**, MPH, Deputy Director, Training, Research and Education for Driving Safety, University of California, San Diego*

With fiscal 2019 High Priority Grant program funding from the Federal Motor Carrier Safety Administration, the Training, Research and Education for Driving Safety (TREDS) program at University of California, San Diego has developed an educational program to reduce the risk distracted driving poses to the commercial motor vehicle industry and all roadway users.

The "Just Drive: Deliver Distraction-Free" course is a one-hour class designed to increase driving safety awareness and decrease distracted driving behaviors among commercial motor vehicle drivers, specifically addressing the use of cell phones and electronic communication devices. The curriculum can be delivered in-person or virtually and utilizes a variety of engagement methods such as PowerPoint®, polling, case examples and video.

Over the past year, TREDS has delivered 11 "Just Drive" train the trainer programs at no-cost to Florida, Georgia, Kentucky, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Texas and Washington, preparing 180 commercial motor vehicle industry and law enforcement professionals to become course instructors. Comments and feedback from the workshop participants have been overwhelmingly positive with many expressing enthusiasm for delivering classes in their respective states.

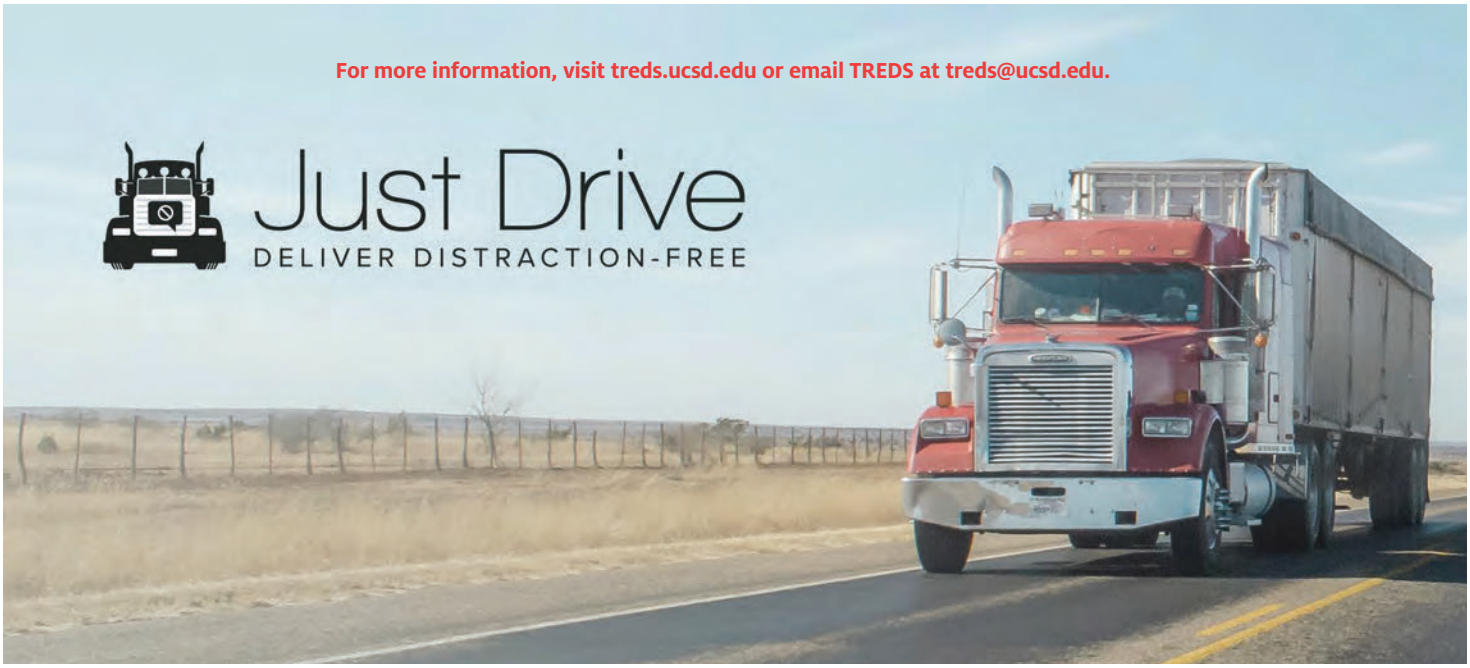
Additionally, 100% of the instructor students agreed that the curriculum adequately covered the risks and consequences of distracted driving and 97% agreed that they planned to use the program.

TREDS has developed support materials to augment the "Just Drive" curriculum, including:

- Social media posts
- Newsletter copy
- Video clips that highlight risks and reinforce safe driving
- A four-minute video comprised of testimonials from commercial driver's license holders that addresses a variety of distracted driving topics (can be viewed on the TREDS website)

Two train the trainer programs, held virtually, will be available in 2022. If you are interested in becoming an instructor, visit the webpages listed below to register.

- Tuesday, May 3, 9-11 a.m. PST
  bit.ly/JustDriveMay2022
- Wednesday, July 13, 10 a.m.-12 p.m. PST
  bit.ly/JustDriveJuly2022 ■





FROM THE DRIVER'S SEAT

Winter Weather Can Be Messy

*By **Byron Bramwell**, Professional Driver, Yellow; America's Road Team Captain*

As a Smith System defensive driving instructor and an America's Road Team Captain, I know the importance of sharing safe-driving techniques with all kinds of drivers. I am a city pickup and delivery driver for Yellow. I have been a professional truck driver for more than 44 years, accumulating 3.3 million safe driving miles.

In my experience, one of the biggest challenges to safe driving that everyone can use more knowledge of is winter weather conditions. As a Missourian, I deal with inclement winter weather several times a year. Here are some tips that have worked well for me year after year:

1. **It's all about YOU.** Getting you to your destination safely is the most important task. You need to be on top of your driving game when taking on bad weather and traffic. Before getting in your vehicle, evaluate your readiness and ask yourself the following:
   - Am I alert?
   - Have I had enough sleep?
   - Do I feel well?

2. **Plan your route and have a Plan B.** Winter weather can make certain roads dangerous, especially if they have not been plowed or properly treated for ice. Plan a backup route. Your normal route may be blocked. When route planning, consider the following:
   - Do I have a good route and a backup planned?
   - Is there terrain that could be challenging in winter weather conditions? For example, is there a big hill on your route? Do you know how to get to your location without having to deal with that dangerous hill?

3. **Give yourself plenty of time to get to your destination.** Leave early so you're not in a rush. Keep as much distance as possible between yourself and other vehicles. The extra time and following distance will allow more time to react to road conditions and keep your stress levels down, allowing for better driving decisions.

   One of the ways I teach this to my students is by challenging them to pretend they are driving on ice during the summer. I have them pretend it is icy and see how far they can go before having to touch their brakes. This makes them look ahead, pace traffic lights and have a large following distance, all while keeping track of their surroundings. Brakes should be carefully applied – just the way you need to drive in bad winter weather. This not only prepares drivers for winter weather driving conditions but also forces them to be better drivers year round.



4. **Make sure your vehicle is in the best condition before hitting the road.** There may not be a safe place to pull over during your trip, so ensuring your vehicle is working properly before leaving will keep you safer. Before starting your vehicle, run your own pre-trip inspection:
   - What is the condition of your car or truck?
   - Is your fuel tank full?
   - Is everything working properly? Lights? Wipers? Tires?
   - Are your windows and mirrors clean?

5. **Stock your vehicle with essential winter weather supplies.** As we saw in early January on I-95 in Virginia, lack of supplies can make a huge emergency worse. People were in a 40+ mile backup for 24 hours or more.

   Before the winter weather hits, stock your vehicle with emergency supplies just in case you get stuck in a similar situation. You never know when you will get caught in a storm. Here are some things I keep in my car and truck:
   - Bottled water
   - Snack food — only keep things that don't perish like granola bars so that supplies can last in your vehicle for a long time
   - Heavy coats, winter hats, blankets, flashlight (check those batteries and keep spares), cell phone and charger, ice scraper, snow shovel, road salt, tow strap, safety vest and safety triangles

If you do get stuck, be very careful of the other traffic around you. They probably don't have full control of their vehicles either.

Remember, the main goal of your trip is to get you there safely. If state and local officials ask you to stay off the roads, it is for your safety and the safety of those working around the clock to make sure our roads are clean, clear and safe to drive on. Follow their guidance.

No trip in winter weather is worth your life. Safe travels and I will see you down the road. ■

Avoid Wheel-Offs with Proper Wheel Maintenance

*By **Jennifer Smith**, e-Commerce Digital Content Specialist, JIT Truck Parts*

While it may sound like something out of Hollywood, road incidents involving wheel separation are all too common. In a 2015 report, the National Transportation Safety Board (NTSB) estimated that an average of 750-1,050 tractor trailer wheel-separation accidents occur per year. This is a real problem. Truck wheels can weigh more than 300 pounds and can cause fatal injuries if they hit other vehicles. According to the NTSB, most trucking wheel-off incidents are due to faulty wheel fasteners, and failing wheel bearings are a prominent secondary cause.

Most manufacturers recommend replacing wheel end components on big rigs every 85,000 to 100,000 miles. Keep reading to learn about the anatomy of a wheel end system, causes of wheel-off conditions, warning signs of failing parts and best-practice maintenance techniques to avoid these potentially dangerous incidents.

The Components of a Wheel End System

Though the main components of a truck wheel end system consist of seals, tapered bearings and a hubcap, there are other bits and pieces, such as spindle nuts and wheel nuts. Those smaller components are equally important and work in unison to provide sufficient lubrication and protection from premature failure while also keeping out unwanted pollutants.

One of the most critical components of the wheel end system is the seal, as it helps to keep grease and oil in the hub. Meanwhile, the hubcap – with or without a center fill plug – side plug and sight window, keep the elements out of the hub (thanks to the seal) and helps to grease the bearings. The bearings consist of a cup, rollers, cage and inner race that must be regularly maintained to avoid misalignment issues under heavy loads. The wheel nuts are designed to provide clamp force while maintaining torque and tension. There are different types of wheel nuts and choosing the right one can help reduce fuel costs, increase the life of the wheel seals and bearings and, most importantly, keep the wheel from loosening and causing wheel-off conditions.

What Causes Wheel-Off Conditions?

The most common cause of incidents is improper installation of wheel nuts which results in a lack of clamping force. If wheel nuts do not have enough torque, they can loosen the wheel. Different nut designs have different requirements, but, when working on hub-piloted wheels, a general rule of thumb is to use a typical M22 x 1.5 stud and 33-millimeter flange nut torqued at 450-500 pounds; however, please consult your manufacturers' manuals for the proper nuts and torque for your truck. The tension between the two materials, called pre-load, can make the difference between movable joints or a clamped force. If a mechanic over-torques nuts, the studs can overstretch and break as well.

Another source of wheel-offs is lack of bearing maintenance. Dried lube or contaminants such as water, road salt or sand in hubcaps can quickly wear out bearings.

Warning Signs of Failing Wheel Ends

Drivers will need to listen, look and feel for the signs of failing wheel bearings, the first of which are hearing squealing, clicking or humming sounds near the tires. These noises could imply that there is a problem with the hub assembly. Uneven tire wear could be another telling sign but could also indicate that the tires are underinflated. Vehicles tugging to the left or right when brakes are applied is another symptom of a bad wheel bearing, as well as a vibrating steering wheel when accelerating at higher speeds. Watch for other signs of issues that can ruin bearings, including heat discoloration from preload, frail rollers and races, and spinning cups and cones.

Wheel End Maintenance

There is a limited service life for any moving truck part. While wheel bearings and other key components may last the vehicle's lifetime, that is hardly ever the case without proper maintenance. This makes servicing hub assemblies a must to avoid bearing issues and wheel separation.

In order to increase longevity, major wheel bearing manufacturers suggest properly lubricating bearings with a clean axle solvent as a starting point for installation. The grease lubricant should have a temperature range between -20 degrees and 325 degrees Fahrenheit. During installation, take care of cups and cones at the same time. While cups and cones may not both fail at once, it is always recommended to replace the components together when one shows signs of damage. Purchasing these products from the same manufacturer will ensure the components are compatible and equipped with the same bearing ratings, material and quality.

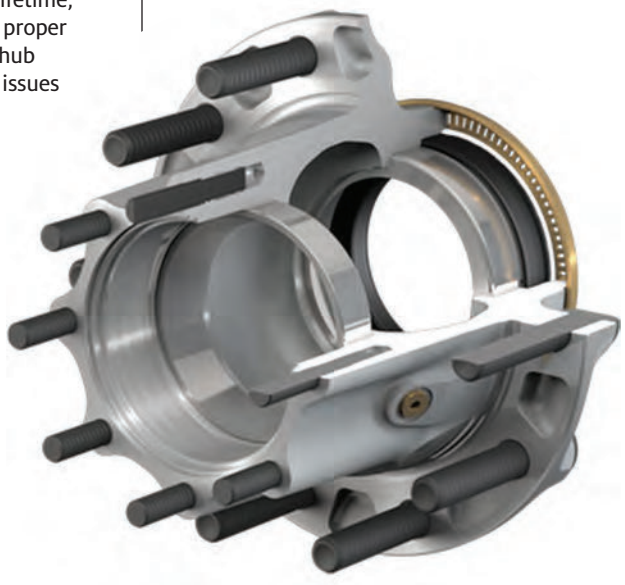
A torque wrench should be used if installing manually adjusted wheel ends, whereas preset wheel ends will have established factory calibrated endplay measurements. The proper endplay measurement for tapered roller bearing adjustment using single or double nut systems on Class 6, 7 and 8 trucks is .001 to .005 inch (.25 to .127 millimeters) in accordance with Technology and Maintenance Council Recommended Practice 618. A dial indicator can determine if adequate endplay was achieved. There should not be much preload, either, as too much could result in excess heat, causing discoloration – one of the symptoms of a failing wheel bearing.

"There is not much room for error in bearing adjustments," said Russ Kolany, heavy-duty key account manager of bearing and seal manufacturer SKF. "Around the thickness of two human hairs is the margin." *(Maintenance Practices to Prevent Wheel-Off Conditions, Fleet Maintenance)*

If the industry standard measurement is not achieved, technicians will need to try again.

Summary

Truck wheel-off incidents cause costly downtime and can be a danger to the driving public. However, they are largely preventable. To reduce the number of these incidents, commercial motor vehicle operators must learn the signs of failing wheel end components and how to properly maintain them for the safety of drivers, passengers and nearby vehicles. ■



The focus area for this year's International Roadcheck, scheduled for May 17-19, is wheel ends. Visit www.roadcheck.org for more information.



Addressing the Nation's Driver Shortage by Cultivating a Driver-First Safety Mindset

By ***Jill Snyder***, *Compliance and Safety Director, Zonar*

Even with continued supply chain disruptions throughout 2020 and 2021, the trucking industry's commitment to delivering essential loads as safely and efficiently as possible remains a top priority. These disruptions have been compounded by an all-time high lack of truck drivers. The American Trucking Associations estimates that the U.S. has about 80,000 fewer drivers than it needs– and that by 2030, the gap could be upward of 160,000.

To meet this challenge, the Biden Administration announced its Trucking Action Plan in December 2021, providing an outline to help recruit top talent in trucking while addressing obstacles to driver retention. The plan streamlines the processing of commercial driver's licenses (CDL), establishes task forces to advance women in trucking (which builds on the recently passed Infrastructure Investment and Jobs Act provision to create a Women of Trucking Advisory Board) and implements additional driver apprenticeship programs – including veteran-focused outreach – to build a strong talent pipeline.

Through the proposed DRIVE SAFE ACT, Congress is also lowering the age requirement for hauling cargo across state lines, allowing drivers to start at age 18, rather than 21. However, this poses yet another challenge: safety-first education for the next generation of drivers along with the continued safety education of veteran truck drivers.

Often fatigue and distracted driving are noted as major causal factors of truck accidents. Truck driver fatigue was found to be associated with 13% of crashes evaluated as part of the Federal Motor Carrier Safety Administration's (FMCSA) Large Truck Crash Causation Study. While lesser known, complacency on the job is another leading factor affecting truck driving safety. In fact, data shows that truck drivers with five to 10 years of experience have more accidents than new drivers due to a complacency mindset.

Therefore, as fleets recruit and train new drivers, they must remember to check in with the veteran drivers too. The trucking industry needs to cultivate a driver-first safety mindset that empowers drivers to follow safety guidelines and checkpoints thoroughly each and every day, providing them with the training, tools and support that builds job satisfaction and keeps our drivers and roads safer.

Put Drivers in the Fleet's Driver Seat

To retain current talent, fleets should find ways to put the driver first in organization-wide decisions. Companies are typically structured with the CEO at the top of the pyramid; however, in the trucking industry, this structure should be inverted to put drivers at the top. Without them hauling deliveries safely and efficiently, no one else would have a job.

Ensure that drivers feel valued and recognized for a job well done. If fleet and safety managers put more emphasis and attention on drivers, these essential workers will likely feel more motivated and experience less monotony on the job.

Technology to Support Driver Rewards

In recent years, more fleets have been providing this type of recognition through high-performer reward and gamification programs. At the end of each trip, the driver's performance is automatically captured from the vehicle's telematics technology. That data is then saved to a scorecard tracked by the fleet manager and the driver. This technology brings the idea of the popular "American Truck Simulator" reward system to the real world.

Alternatively, some fleets are changing their payment models to drive more incentive among employees. Rather than payment on a per-mile basis, organizations are shifting to a per-hour basis or a salary base to accommodate for stall time if a load isn't ready for a truck. Previously, issues with stall time would lead to reduced pay and result in a higher turnover rate as drivers looked elsewhere for more consistent payments for each hour they work. Another example is an auto carrier fleet that would pay drivers per car loaded. At the end of the year, the drivers were able to keep whatever money was left after damages were paid.

Reducing False Accusations for Drivers

Carriers are also using technology to better protect drivers from false accusations in the case of a crash. When any commercial motor vehicle is involved in an incident, the ramifications are complicated. Commercial



drivers' safety records are examined, legal resources are rallied and many drivers feel on the defense from nearly every direction – even if they did nothing wrong.

In the event of an accident, vehicles with smart dashcam technology, such as coaching systems, can capture video evidence in real-time to see when, where and how the incident occurred. There is also a challenge feature to exonerate drivers with safe-driving behavior.

No matter how safe or experienced a driver is, one bad day can ruin a career. Commercial fleets are especially vulnerable to lawsuits. We all have seen stories of the nuclear verdicts against commercial carriers involved in accidents and the impact it has on the industry. Telematics and dashcam footage provide objective evidence that can help protect a driver's career, and a carrier's bottom line, by proving who is at fault. Receiving this level of protection from an employer can further increase driver loyalty, making it more likely that they will stay on for the long term.

Safety Is a Full Fleet Responsibility

Finally, remember that safety isn't just the responsibility of the drivers, but also the dispatchers and management. Open the dialogue across the organization about safety expectations and procedures – and ask the drivers themselves what works best for them on the job. Management should consult drivers on any new telematics, in-cab coaching solutions or other devices they are considering implementing across the fleet.

According to FMCSA, large truck-related accidents have steadily increased by as much as 20% since 2015 and the World Health Organization projects that by 2030 road crashes are expected to become the fifth leading cause of death worldwide. To change these statistics, we need to make a change in the trucking culture to cultivate a driver-first safety mindset. This will not only reduce accidents and keep drivers safe, but it will also help to retain driving talent, which is key to limiting the growing truck driver shortage. Through initiatives like the Trucking Action Plan, the federal government is taking action to strengthen America's trucking workforce. Fleets and vendor organizations must also do their part to support our drivers every step of the way. ■

Kodiak Robotics Names Brett Fabbri as Head of Law Enforcement Policy and Roadway Safety

Brett Fabbri, former chair of CVSA's Enforcement and Industry Modernization Committee and former California Highway Patrol (CHP) assistant division commander for the Enforcement and Planning Division, joined Kodiak Robotics Inc., a self-driving trucking company. He now serves as the head of law enforcement policy and roadway safety.

Fabbri will oversee Kodiak's relationships with law enforcement agencies across all 50 states, while helping to ensure Kodiak trucks continue to meet the company's rigorous standards and rules of the road prior to driverless deployment on the highway. Additionally, Fabbri will work with national law enforcement leaders to adapt to trucking regulations and policies, making certain that Kodiak autonomous trucks are safe and well-maintained vehicles.

"Brett's role is vital to Kodiak as we work to launch autonomous truck operations across the United States," said Don Burnette, founder and CEO of Kodiak Robotics. "Brett brings valuable highway safety insights and experience to the Kodiak team which will be crucial to the commercial launch of self-driving trucks. Working closely with law enforcement is critical to making autonomous driving technology available at scale."

Fabbri spent more than two decades working for the CHP. Most recently, he served as the assistant division commander for the Enforcement and Planning Division at CHP headquarters. In this role, he oversaw the Commercial Vehicle Section and Collision Investigation Unit, which are responsible for autonomous vehicle technology for heavy-duty, light-duty and passenger vehicles.

"I joined the Kodiak Robotics team because I believe in autonomous trucking's potential to save lives," said Fabbri. "During my 23-year tenure at California Highway Patrol, I witnessed the safety hazards on our public roads and the resulting devastation that rippled throughout the nation. Autonomous trucking will make our roads safer for all drivers and Kodiak Robotics is at the forefront of this innovation."

Prior to his retirement from CHP, Fabbri also chaired CVSA's Enforcement and Industry Modernization Committee, which identifies technological advancements that can be leveraged to improve commercial motor vehicle safety. In April 2021, he was appointed to the American Transportation Research Institute as a research advisory committee member. This advisory committee is composed of government officials, independent scientists, labor union officials, academics and trucking company executives and suppliers from a diverse cross-section of the industry, all who understand the importance of sound science to an industry as complex as the trucking industry.

Fabbri is one of several new team members Kodiak has added as the company aims to double its staff in 2022. ■

Kodiak Robotics Inc. was founded in 2018 to develop autonomous technology that carries freight forward so that people, partners and the planet can thrive. Kodiak is making the freight industry safer and more efficient by building and operating self-driving trucks designed to operate on highway routes. Kodiak delivers freight daily for its customers between Dallas-Fort Worth and Houston, operating autonomously on the highway portion of the route. In January 2021, Kodiak became the first company in the autonomous trucking industry to announce disengage-free customer deliveries, releasing footage of more than 1,000 miles of disengage-free driving. Learn more about Kodiak on the web at www.kodiak.ai.

About 'RAD Inspection News'

'RAD Inspection News' features news and other stories pertaining to the North American Standard Level VI Inspection Program for transuranic waste and highway route controlled quantities (HRCQ) of radioactive material. This inspection is for select radiological shipments that include enhancements to the North American Standard Level I Inspection Program and the North American Standard Out-of-Service Criteria with added radiological requirements for transuranic waste and HRCQ of radioactive material.

Learn more about the Level VI Inspection Program at www.cvsa.org.

'RAD Inspection News' is made possible under a cooperative agreement with the U.S. Department of Energy. Since January 2007, it has run as a section inside CVSA's "Guardian." ■



Waste Isolation Pilot Plant 2021, at a Glance

*By **Bobby St. John**, Deputy Manager, Communications, WIPP*

The Waste Isolation Pilot Plant (WIPP) is the only operating deep geologic repository for transuranic waste in the world and has been a key component of the cleanup of the U.S. Department of Energy (DOE) Environmental Management's (EM) legacy sites throughout the U.S.

During 2021, WIPP continued to provide support for the EM mission, while at the same time making significant progress on major infrastructure and recapitalization projects onsite. WIPP averaged approximately five shipments per week during 2021, receiving 210 shipments throughout the calendar year. This included safely transporting transuranic (TRU) waste more than 230,000 miles from generator sites to the WIPP facility for disposal.

WIPP reached other transportation-related milestones during 2021, receiving the 13,000th shipment of TRU waste since beginning operations in 1999 and traveling more than 15.5 million loaded miles safely, since the beginning of the program (see page 37 for more information). WIPP plans to increase the number of shipments received in 2022, targeting an average of 10 shipments per week.

WIPP continues to be the cornerstone of the DOE cleanup mission and WIPP workers managed several other significant accomplishments during 2021, one of the most important being the completion of mining in Panel 8. Panel 8 is expected to be fully outfitted and ready for waste emplacement approximately three months prior to Panel 7 being filled, ensuring no interruption in the flow of TRU waste shipments to WIPP.

In addition, contractors for the two major capital asset projects – the utility shaft and safety significant confinement ventilation system – continued to make significant progress on construction work. In late 2021, WIPP received approval from the New Mexico Environment Department for a Class 3 permit modification needed to complete the mining of the new utility shaft which, in conjunction with the safety significant confinement ventilation system, will provide a much-needed increase in airflow to the WIPP underground, allowing mining, maintenance and waste emplacement to occur simultaneously, which is not possible under the current airflow rates. ■



Waste Isolation Pilot Plant Receives 13,000th Shipment

The U.S. Department of Energy (DOE) Environmental Management's Waste Isolation Pilot Plant (WIPP) received its 13,000th shipment of transuranic (TRU) waste in November 2021. This marks an important milestone in DOE's mission to clean up the country's Cold War legacy.

"This accomplishment reflects the hard work and dedication of our workers and contractors," said William "Ike" White, acting assistant secretary for DOE's Office of Environmental Management. "It also demonstrates the department's commitment to future generations as we continue our cleanup mission as safely and quickly as possible."

The 13,000th shipment, which consisted of defense-generated contact-handled TRU waste, arrived at WIPP on Nov. 11, 2021. The shipment came from DOE's Advanced Mixed Waste Treatment Project in Idaho, which has accounted for about half of the shipments – more than 6,605 to date – WIPP has received. Eight shipments arrived at WIPP in one recent week, including two from Los Alamos National Laboratory in New Mexico.

TRU waste, a byproduct of the nation's nuclear defense program, consists of tools, rags, protective clothing, sludge, soil and other materials contaminated with radioactive elements that have atomic numbers greater than uranium. Most of the 13,000 shipments were of contact-handled TRU waste, which does not require shielding to safely handle, transport and emplace. A total of 775 remote-handled (RH) waste shipments have been shipped to WIPP. The majority of RH waste containers are handled in shielded facility casks and emplaced in the walls of the underground repository due to their higher radiation dose rates.

Every WIPP shipment of TRU waste meets all U.S. Department of Transportation requirements and WIPP's drivers must pass stringent training requirements. Shipment protocols were developed through cooperative efforts with states, tribal governments and the DOE. Shipments are also monitored via satellite at all times. To date, WIPP drivers have logged more than 15.5 million safe miles without a serious injury or release of radioactive material.

WIPP's first shipment came from Los Alamos National Laboratory on March 26, 1999. Other milestone shipments have included the final shipment from the Rocky Flats Environmental Technology Site in 2005, the first shipment of remote-handled waste in 2007 and the 10,000th contact-handled waste shipment in 2011, also from Idaho. Since TRU waste disposal operations began at WIPP, 22 sites in the DOE complex have been cleaned up, reducing risk to millions of Americans.

"WIPP continues to be the cornerstone of DOE's efforts to reduce the defense legacy TRU waste footprint," said Reinhard Knerr, manager of the Carlsbad Field Office that oversees WIPP and the National Transuranic Program. "WIPP's transportation program has been a tremendous success and I congratulate everyone involved on a job well done."

WIPP is a DOE facility designed to safely isolate defense-related TRU waste from people and the environment. Waste temporarily stored at sites around the country is shipped to WIPP and permanently disposed in rooms mined out of an ancient salt formation 2,150 feet below the earth's surface. WIPP is located 26 miles outside of Carlsbad, New Mexico. ■

2022 Level VI Certification Training Schedule

Under a cooperative agreement with the U.S. Department of Energy, CVSA offers Level VI Inspection certification courses for inspectors to become trained and certified to conduct inspections of drivers and vehicles transporting transuranic waste and highway route controlled quantities of radioactive material. Level VI Inspection certification training is available to jurisdictional inspectors who are certified in North American Standard Part A (driver) and Part B (vehicle) and General Hazardous Materials.







Based on demand, CVSA will host virtual Level VI Inspection certification classes, as needed.

Any jurisdiction interested in Level VI Inspection certification training or with facilities to host a course is asked to contact CVSA Director of Level VI Inspection Program Carlisle Smith at carlisles@cvsa.org or 301-830-6147.

Longtime Level VI Inspection Program Advocate Gaylon Fuller Passes Away

*By **Carlisle Smith**, Director of Level VI Inspection Program, Commercial Vehicle Safety Alliance*

The Level VI Inspection Program lost a true friend and advocate last December with the passing of Gaylon Fuller. Fuller's involvement with the Level VI Inspection Program spanned more than 15 years while serving as the Waste Isolation Pilot Plant project manager for CAST Transportation.

Fuller loved music and the outdoors, and made good use of his Harley to see as much of the latter as he could. He was always quick to assist the Level VI Inspection Program in any way. His warm and gregarious personality made him a perfect fit with many of the Level VI national instructors and directors over the years.

Fuller is survived by his parents, Charles Phillip and Lois; siblings Wesley and Lara Ann; and his children Gentry and Shaylee. Nieces and nephews include Makayela, Dustin, Chase, Bailee, Cortlin, Caleb, Abigail and great-niece Danielle.

Fuller attended Cloudcroft Municipal School, New Mexico State University and the Firefighter's Training Academy in Socorro, New Mexico.

After graduating the police academy in Silver City, his first post in law enforcement was as a patrol officer in Hurley, New Mexico. Fuller next accepted a position with the Roswell Police Department, and while there, he married Lacee Huffmon in 1995. He soon transitioned from the police force to work as a U.S. Department of Transportation law enforcement officer for the state of New Mexico.

He later accepted a project/terminal manager position with CAST Transportation, which in 2018 led to his role as a training specialist with Nuclear Waste Partnership LLC.

Throughout his life, Fuller's passion and enthusiasm for volunteer fire prevention touched every aspect of his being. First volunteering at the Mayhill Volunteer Fire Department (VFD), Fuller later helped establish the Upper Cox Canyon VFD. Once settled in Carlsbad, Fuller re-entered the volunteer fire department field when he joined the La Huerta VFD. This led to his recruitment as Happy Valley VFD chief.

His legacy will live on in the hearts and minds of everyone he interacted with, as well as the communities he was so dedicated to serving. The Level VI Inspection Program shall truly miss you, old friend. ■



Level VI Roadside Inspections (2022 - Fiscal)

LEVEL VI INSPECTIONS	Federal	State	Total	% of Total
Number of Level VI Inspections	0	176	176	100%
Point of Origin	0	98	98	55.68%
En Route	0	78	78	44.32%
Point of Destination	0	0	0	0%
Unknown Location	0	0	0	0%
Level VI Inspections with No Violations	0	172	172	97.73%
Level VI Inspections with Violations	0	4	4	2.27%
Level VI Inspections with Out-of-Service Conditions	0	2	2	1.14%

Level VI Roadside Inspection Violations (2022 - Fiscal)

Violation Code	Violation Description	# of Inspections	# of Violations	% of Total Violations	# of OOS Violations	OOS %
393.45B2	Brake Hose or Tubing Chafing and/or Kinking	2	2	50.00%	2	66.67%
177.817A	No or Improper Shipping Papers (carrier)	1	1	16.67%	0	0%
397.101D	No or Incomplete Route Plan for Radioactive Materials	1	1	16.67%	0	0%
172.310D	Type B, B(U), B(H) Package Not Marked with Radiation Symbol	1	1	16.67%	0	0%

CVSA LEADERSHIP

BOARD OF DIRECTORS

PRESIDENT
Capt. John Broers
South Dakota Highway Patrol

VICE PRESIDENT
Maj. Jeremy "Chris" Nordloh
Texas Department of Public Safety

SECRETARY
Col. Russ Christoferson
Montana Department of Transportation

PAST PRESIDENTS
Sgt. John Samis
Delaware State Police

Lt. Donald Bridge Jr.
Connecticut Department of Motor Vehicles

REGION PRESIDENTS

Region I
Tpr. William Alarcon
New Jersey State Police

Region II
Capt. Bart Teeter
Texas Department of Public Safety

Region III
Maj. Jon E. Smithers
Indiana State Police

Region IV
Brad Marten
Montana Department of Transportation

Region V
Richard Roberts
British Columbia Ministry of Transportation and Infrastructure

REGION VICE PRESIDENTS

Region I
Tpr. James Thomas
Rhode Island State Police

Region II
Lt. Ronald Jenkins
Oklahoma Highway Patrol

Region III
Lt. Mike Maytum
Nebraska State Patrol

Region IV
Tpr. Jeremy Disbrow
Arizona Department of Public Safety

Region V
Krista Cull
Newfoundland and Labrador Transportation Regulation Enforcement

LOCAL PRESIDENT
Ofc. Thomas Mrozinski, Jr.
Frisco (Texas) Police Department

LOCAL VICE PRESIDENT (INTERIM)
Ofc. Lincoln Sweeney
Cedar Hill (Texas) Police Department

NON-VOTING LEADERSHIP

ASSOCIATE MEMBER PRESIDENT
Andrea Sequin
Schneider

ASSOCIATE MEMBER VICE PRESIDENT
Derek Barrs
HNTB Corporation

COMMITTEE CHAIRS

Crash Data and Investigation Standards Committee
Capt. Bryant Gay
Florida Highway Patrol

Driver-Traffic Enforcement Committee
Capt. Chris Barr
Indiana State Police

Enforcement and Industry Modernization Committee
Capt. Leonard Dittman
Colorado State Patrol

Hazardous Materials Committee
Sgt. Brad Wagner
Nebraska State Patrol

Information Systems Committee
Holly Skaar
Idaho State Police

Passenger Carrier Committee
Tpr. William Alarcon
New Jersey State Police

Policy and Regulatory Affairs Committee
Capt. John Hahn
Colorado State Patrol

Size and Weight Committee
Brad Marten
Montana Department of Transportation

Training Committee
Lt. Ronald Jenkins
Oklahoma Highway Patrol

Vehicle Committee
Tpr. John Sova
North Dakota Highway Patrol

PROGRAM CHAIRS

Cooperative Hazardous Materials Enforcement Development
Sgt. Kevin Hogan
Michigan State Police

Human Trafficking Prevention
Lt. Col. Michael Krumm
Michigan State Police

International Driver Excellence Award
Brett Graves
Maverick Transportation, LLC

International Roadcheck
Maj. Michael Forman
Mississippi Department of Transportation

Level VI Inspection
M/Sgt. Todd Armstrong
Illinois State Police

North American Cargo Securement Harmonization Public Forum
Tpr. Jeremy Disbrow
Arizona Department of Public Safety

North American Inspectors Championship
Richard Roberts
British Columbia Ministry of Transportation and Infrastructure

Operation Airbrake
Lt. Aaron Hayden
Maine State Police

Operation Safe Driver
Capt. Jon Olsen
Minnesota State Patrol

PBBT Users
Lt. Joseph Greene
Kansas Highway Patrol

CVSA SPONSORS

PREMIER

FedEx

iis intelligent imaging systems Drivewyze

DIAMOND

amazon

ird INTERNATIONAL ROAD DYNAMICS INC.

PrePass SAFETY ALLIANCE

PLATINUM

Greyhound

J. J. Keller & Associates, Inc. Since 1953

SCHNEIDER

YELLOW

GOLD

ABF Freight

AAMVA

JBHC

kapsch challenging limits

LANDSTAR

MICHELS

NORPASS North American Preclearance and Safety System

Omnitracs

R+L CARRIERS Your Global Transportation Provider

TRUCKING ALLIANCE

U-HAUL

CVSA SPONSORS

SILVER

American Bus Association
Austin Powder Company
Brake Tech Tools
Cargo Transporters Inc.
EROAD Inc.
Great West Casualty Company
Kenan Advantage Group Inc.
MANCOMM Inc.
United Motorcoach Association
US Ecology
Werner Enterprises Inc.

BRONZE

Acuity Insurance
American Pyrotechnics Association
Coach USA
DATTCO Inc.
Direct ChassisLink Inc.
Independent Carrier Safety Association
Vehicle Inspection Systems Inc.
Zonar Systems

FRIENDS OF CVSA

Certarus
J.E.B. Environmental Services LLC
Linde Gas & Equipment Inc.
Lytx
PITT OHIO
Price Benowitz Injury Lawyers LLP
Railsback HazMat Safety Professionals LLC
Washington Trucking Associations

Welcome

TO OUR NEW ASSOCIATE MEMBERS

As of March 31, 2022

All State Tank Lines Inc. / ABS Fuel Systems LLC / Aevitas Inc. / AWM Consulting Services / Clark Freight Lines Inc. / Holland LP
Jillamy Heavy Haul LLC / MobileMed Transportation Inc. / Pressure Systems International / Retail Business Services / Riverside Transportation Inc.
SafetyPro Consulting LLC / Salem Carriers/Salem Leasing / Torc Robotics Inc. / TransX Group of Companies / Trolleys Inc dba Sunway Charters
Vogel Disposal Service Inc. / Yankee Line

COMMERCIAL VEHICLE SAFETY ALLIANCE
CVSA
6303 Ivy Lane, Suite 310
Greenbelt, MD 20770-6319



After two years off due to the pandemic, CVSA is excited to resume its North American Inspectors Championship, the only event that tests, recognizes and awards commercial motor vehicle inspector excellence. **This year's championship is scheduled for Aug. 15-19 in Indianapolis, Indiana.**

Visit www.cvsa.org/events/north-american-inspectors-championship for more information.

Quotation

Number

MSP081822.1

Bay State Alarm Security, Inc. * 462 Pleasant Street * Mar boro, MA 01752 Ph 508-485-1174 Fax 508-624-6568

To:	**Massachusetts State Police**	**Date: August 18th, 2022**
	Division of Homeland Security	
	470 Worcester Road	Facility: State Police
	Framingham, MA 01702	Contact: Sgt. Noah Pack
From:	James P McStay Sr.	
		Job: Provision of ALPR Trailer Components
Re:	ALPR Trainer Components	

#	QTY	U/M	DESCRIPTION	UNIT	AMOUNT
1.	12	Ea	FC574250000 – NEOLOGY P525 CAMERA	7449.70	89396.40
2.	3	Ea	HC350244L010 – NEOLOGY P525 POWER & SERIAL CABLE (10M)	405.46	1216.38
3.	9	Ea	HC350242L010 – SINGLE ETHERNET CABLE (10M)	227.00	2043.00
4.	12	Ea	HW25X0011 – NEOLOGY MOUNTING BRACKET	232.65	2791.80
5.	12	Ea	INJ-C201G-BT-24-T – ANTAIRA POE INJECTOR	453.00	5436.00
6.	1	Ea	TRACO TEP 100-1218 12VDC TO 48VDC POWER SUPPLY	250.00	250.00
7.	4	Ea	MEAN WELL RS-1000-48 – 110VAC TO 48VDC POWER SUPPLY	80.00	320.00
8.	8	Ea	FC4819730200 – NEOLOGY P497 CAMERAS	4819.00	38552.00
9.	8	Ea	HC350228L005 – NEOLOGY GLANDED 5M CABLE FOR P497	255.00	2040.00
10.	8	Ea	P497MOUNT – MOUNTING BRACKET FOR P497 CAMERA	200.00	1600.00
11.	6	Ea	DDR-60G-15 – MEAN WELL 15VDC, 60W DC/DC CONVERTER	47.50	285.00
12.	8	Ea	RHINO PSE15-160 – 110VAC TO 15VDC POWER SUPPLY	150.00	1200.00
13.	7	Ea	RV55 – SIERRA WIRELESS RV55 ROUTER	864.53	6051.71
14.	14	Ea	FXUB66.01.0150C – TAOGLAS MAXIMUS FLEXIBLE ANTENNA (SMA)	3.40	47.60
15.	2	Ea	LNX-500A-T – ANTAIRA 12VDC, 10/100 SWITCH	165.00	330.00
16.	1	Ea	BSA TOOL KIT – HAND TOOLS AND SOCKET SET KIT	400.00	400.00
17.					0.00
18.					0.00
19.					0.00
20.					0.00

GSA Advantage!

Signature Please

TOTAL	151959.89
TAX	0.00
S&H	0.00
GRAND TOTAL	$151,959.89

NOTES:

1. **Prices quoted are valid for 30 days**
2. **Equipment warranty one year**
3. **Please sign and return a copy to Bay State Alarm Security, Inc.**

REKOR
INTELLIGENCE DRIVEN INNOVATION

Rekor Edge Max



MOUNTABLE LICENSE PLATE & VEHICLE RECOGNITION

Rekor Edge Max is a complete vehicle recognition solution. Engineered for high-speed primary roadways and highways, Ed Max seamlessly captures and processes vehicle data on-device from advanced distances. The system features a durable enclos onboard modem, easy mounting, optional solar power, and can even be configured with two cameras to increase capture range.

FEATURES AND FUNCTIONS

OPERATION READY

- 3-4 lanes, 300 ft max range*
- 120 mph max capture speed
- Easily mount to a pole or surface for quick installation
- Complete vehicle recognition & processing solution

STATE-OF-THE-ART RECOGNITION

- Advanced vehicle recognition with plate, make, type, color, and direction of travel
- Accurate in day/night and all-weather conditions
- Read paper, temporary, and vanity plates
- Real-time alerting

POWERFUL PERFORMANCE

- 1920 x 1080 HD Camera
- Outdoor rated, IP66, NEMA4
- 4G LTE, Ethernet ready
- Rekor Scout™ ready**
- Scout dashboard available in the cloud or on-premise
- Optional solar power and/or pole

*Dual camera solution available for increased lane coverage.
**Rekor Scout™ is a proprietary software platform for accessing and analyzing Edge captured vehicle data.

REKOR EDGE SPECIFICATIONS

Recommended usage

Use cases:	Highways, Primary Roads

Coverage*

Lane coverage:	3-4 lanes (5-6 lanes with dual cameras)
Distance:	300 ft max
Speed:	120 mph max

Camera specifications

Camera resolution:	1920 x 1080 HDTV 1080p
Image compression:	JPEG
Video streaming:	H.264
Network security:	Password, IP address filtering
IR illumination:	Optimized IR w/power efficient, long-life 850 nm IR LED's
Rekor Scout™ features:	Search (e.g. partial plates, no plates, vehicle characteristics), hotlists, alerts, reports, data security/sharing, and much more

Communications

Communications:	Ethernet, Cellular Modem
Cellular modem:	3G, 4G LTE MIMO
Cellular service:	Not included
GPS:	Included
Security:	SSL over websockets & HTTPs

Mount & power

Mounting style:	Surface or Pole
Input voltage range:	9 VDC - 48 VDC
Power consumption:	Average: 18W, Max: 22W

Available accessories (additional charges apply)

Mounting pole:	19.6 ft | above ground: 14 ft, depth: 5-6 ft
Solar power:	39x66x1.3 in array

Environmental specifications

Enclosure:	Diecast aluminum, IP66
Operational temperature:	-22°F to 131°F
Storage temperature:	-40°F to 149°F
Warranty:	Full repair/replace available

*Maximum coverage values. Actual performance may vary.



REKOR®
INTELLIGENCE DRIVEN INNOVATION

Ready to get started?
Contact sales@rekor.ai

www.rekor.ai 410.762.0800

24THE COMMONWEALTH OF MASSACHUSETTS

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY

DEPARTMENT OF STATE POLICE

470 WORCESTER ROAD
FRAMINGHAM, MA 01702

Request for Response (RFR)

Document Title: Firearms, Ammunition, Less Lethal Munitions, and Related Accessories, Training and Services

COMMBUYS Bid#: BD-22-1084-POLGH-GHQ-65259

Agency Document Number SP22-AMMO-X86
August 6, 2021

Please Note: This is a single document associated with a complete Bid (also referred to as Solicitation) that can be found on www.COMMBUYS.com. All Bidders are responsible for reviewing and adhering to all information, forms and requirements for the entire Bid, which are all incorporated into the Bid. Bidders may also contact the COMMBUYS Helpdesk at COMMBUYS@state.ma.us or the COMMBUYS Helpline at 1-888-MA-STATE. The Helpline is staffed from 8:00 AM to 5:00 PM Monday through Friday Eastern Standard or Daylight time, as applicable, except on federal, state and Suffolk county holidays.

THIS PROCUREMENT IS COVERED BY THE WORLD TRADE ORGANIZATION GOVERNMENT PROCUREMENT AGREEMENT (WTO/GPA)

REQUEST FOR RESPONSE
RFR #SP22-AMMO-X86
COMMBUYS Bid # BD-22-1084-POLGH-GHQ-65259

1 RFR INTRODUCTION AND PROCURMENT SCOPE AND DESCRIPTION…….. 1
1.1 Applicable Procurement Law …….. 1
1.2 Acquisition Method …… 1
1.3 Whether Single or Multiple Contractors are Required for this Contract ……..1
1.4 Entities Eligible to Use the Resulting Contract …….. 2
1.5 Expected Duration of Contract …… 2
1.6 Anticipated Expenditures, Funding or Compensation …… 2
1.7 Basis for estimated dollar value for this Contract …….. 3
1.8 Basis for estimated number of units for this Contract …….. 3

2 ESTIMATED PROCUREMENT CALENDAR . ……3
2.1 Written questions via the Bid Q&A on COMMBUYS …….. 3
2.2 Locating Bid Q&A ……..…… 4
2.3 Amendment Deadline……... 4

3 SPECIFICATIONS …… 4

4 OTHER TERMS …… 8
4.1 Contractors Terms & Conditions ……... 8
4.2 Reporting …….. 8
4.3 Contract Management ……... 9
4.4 Change Notification …… 9
4.5 Invoices and Payments …….. 9
4.6 Contract Amendments …….. 10
4.7 Contract Renewals …….. 10
4.8 Performance Measures……. ……... 10
4.9 Insurance……..…… 11
4.10 Contract Termination for Convenience ……..... 11
4.11 Contract Termination for Cause …….. 11

5 EVALUATION CRITERIA …….. 12

6 INSTRUCTIONS FOR SUBMISSION OF RESPONSES …….. 13
6.1 Required Forms …….. 14

7 APPENDIX 1 – REQUIRED TERMS FOR ALL RFRS …….. 15

8 APPENDIX 2 – RFR REQUIRED SPECS …… 17

9 APPENDIX 3 – INSTRUCTIONS FOR EXECUTION AND SUBMISSION OF COMMONWEALTH STANDARD FORMS …….. 22

10 APPENDIX 4 – GLOSSARY …….. 25

RFR INTRODUCTION AND PROCUREMENT SCOPE AND DESCRIPTION

This solicitation is to establish and award a contract(s) to provide the Massachusetts State Police, the Massachusetts Department of Correction, and the Massachusetts Environmental Police with weapons, ammunition, targets, repair/replacement parts, cleaning kits, related accessories, and all related firearm training and certification classes for regular and tactical operations and "less lethal" munitions.

Electronic Quote Submission Instructions

Bidders are advised that Massachusetts State police (1) restricts submission of written questions to the Bid Q&A tool and (2) requires all responses to be submitted using the online submission tools available to active COMMBUYS account holders only. Bidders are solely responsible to monitor this site for Bid amendments, if any. Bidders may monitor the record by frequently checking the Header Information for the list of Amendments. Bidders with active COMMBUYS accounts may also monitor the record through COMMBUYS email notification and record tracking tools enabled when a vendor acknowledges receipt of a bid. To establish a COMMBUYS account, bidders must select the Register link on www.commbuys.com and complete the online subscription process.

1.1 Applicable Procurement Law

Check Appropriate Box ("X"):	Type of Purchase	Applicable Laws
	Executive Branch Goods and Services	
☒	Goods and Services	MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00
☐	Human and Social Services	MGL c. 7, § 22, § 22N; c. 30, § 51, § 52; 801 CMR 21.00; 808 CMR 1.00
☐	Legal Services	MGL c. 30, § 51, § 52 and § 65; c. 7, § 22; and 801 CMR 21.01(2) (b)
☐	Grants	MGL c. 7A, § 7; St. 1986 c. 206, § 17; 815 CMR 2.00

1.2 Acquisition Method:

Check All Applicable ("X"):	Category
☒	Fee-For-Service. This is a rate contract.

1.3 Whether Single or Multiple Contractors are Required for Contract:

Check One ("X"):	
☐	Single Contractor
☒	Multiple Contractors

a. Estimated Number of Awards

The Department seeks multiple contractors. The intent of this RFR is to establish and maintain a list of qualified contractors from which the Department, and the other Commonwealth Agencies defined as eligible entities, can select.

b. Adding Contractors after initial Contract Award

This is an Open Enrollment Contract. Under the open enrollment process, the RFR may be re-opened at any time if deemed necessary by the Strategic Sourcing Team, allowing bidders to respond at any point during the life of the solicitation. However, all contracts resulting from this RFR will expire simultaneously. The Department will not accept new bids that are received less than 6 months away from the maximum and final end date of the solicitation. The Department makes no guarantee that any commodities or services will be purchased from any contract resulting from this RFR.

1.4 Entities Eligible to Use the Resulting Contract

Any contract(s) resulting from this Bid will be open for use by the State Police, the Department of Correction, the Environmental Police, as well as other Executive Branch agencies that fall within the Executive Office of Public Safety and Security (EOPSS). Contracts are also open for use by Massachusetts Sheriff's offices.

EOPSS agencies and Sheriff's offices interested in using this contract may submit a request to the issuing agency and will be responsible for executing their own contracts/purchase orders and paying their own invoices for goods and/or services acquired from this Contract.

1.5 Expected Duration of Contract (Initial Duration and any Options to Renew):

Contract Duration	Number of Options	Number of Years/Months
Initial Duration		**Up to 36 months**
Renewal Options	**Three (3)**	**Up to (3) 12 month options**
Total Maximum Contract Duration		**6 years**

1.6 Anticipated Expenditures, Funding or Compensation:

Expenditures are estimated at $7,500,000.00 for the life of the contract based on previous expenditures. This is for informational purpose only.

If additional funds become available during the contract duration period, the department reserves the right to increase the maximum obligation to contract executed as a result of this RFR, subject to available funding, satisfactory contract performance and service or commodity needed, for MSP sites not specifically listed.

Contract prices will remain fixed during the initial contract period. Contractors will have an opportunity to request a price increase if an option to renew is offered. Contractors will need to submit written justification and supporting documentation with price increase requests. The Department of State Police does not guarantee that increase requests will be granted.

1.7 Basis for estimated dollar value for this Contract (including all options to renew)
The "Estimated Value (US$)" for this Bid was based on the previous year's expenditures

1.8 Basis for estimated number of units for this Contract (including all options to renew)
The "Estimated Units" for this Bid was based on previous year's expenditures.

Any estimates or past procurement volumes referenced in this Bid are included only for the convenience of Bidders, and are not to be relied upon as any indication of future purchase levels.

2 ESTIMATED PROCUREMENT CALENDAR

EVENT	DATE
Bid Release Date	August 6, 2021
Deadline for Submission of Questions through COMMBUYS "Bid Q&A"	August 27, 2021
Official Answers for Bid Q&A published (Estimated)	September 7, 2021
Deadline for Quotes/Bid Responses ("Bid Opening Date/Time" in COMMBUYS)	Initial bids due by September 20, 2021 3:00 PM EST. Open enrollment bids are due no later than April 30, 2027.
Notification of Apparent Successful Bidder(s) (Estimated)	The week of October 26, 2021
Estimated Contract Start Date	November 1, 2021

Times are Eastern Standard/Daylight Savings (US), as displayed on the COMMBUYS system clock displayed to Bidders after logging in. If there is a conflict between the dates in this Procurement Calendar and dates in the Bid's Header, the dates in the Bid's Header on COMMBUYS shall prevail. Bidders are responsible for checking the Bid record, including Bid Q&A, on COMMBUYS for Procurement Calendar updates.

2.1 Written questions via the Bid Q&A on COMMBUYS
The "Bid Q&A" provides the opportunity for Bidders to ask written questions and receive written answers from the SST regarding this Bid. All Bidders' questions must be submitted through the Bid Q&A found on COMMBUYS (see below for instructions). Questions may be asked only prior to the Deadline for Submission of Questions stated in the Estimated Procurement Calendar. The issuing department reserves the right not to respond to questions submitted after this date. It is the Bidder's responsibility to verify receipt of questions. Additionally, the Department reserves the right to, in its sole discretion, to not answer all questions submitted by Bidders. It is the Bidder's responsibility to verify the receipt of questions and clarification requests.

Please note that any questions submitted to the SST using any other medium (including those that are sent by mail, fax, email or voicemail, etc.) will not be answered. To reduce the number of redundant or duplicate questions, Bidders are asked to review all questions previously submitted to determine whether the Bidder's question has already been posted.

Bidders are responsible for entering content suitable for public viewing, since all of the questions are accessible to the public. Bidders must not include any information that could be considered personal, security sensitive, inflammatory, incorrect, collusory, or otherwise objectionable, including information about the Bidder's company or other companies. The SST reserves the right to edit or delete any submitted questions that raise any of these issues or that are not in the best interest of the Commonwealth or this Bid.

All answers are final when posted. Any subsequent revisions to previously provided answers will be dated.

It is the responsibility of the prospective Bidder and awarded Contractor to maintain an active registration in COMMBUYS and to keep current the email address of the Bidder's contact person and prospective contract manager, if awarded a contract, and to monitor that email inbox for communications from the Purchasing Department, including requests for clarification. The Purchasing Department and the Commonwealth assume no responsibility if a prospective Bidder's/awarded Contractor's designated email address is not current, or if technical problems, including those with the prospective Bidder's/awarded Contractor's computer, network or internet service provider (ISP) cause email communications sent to/from the prospective Bidder/Awarded contractor and the Purchasing Department to be lost or rejected by any means including email or spam filtering.

2.2 Locating Bid Q&A

Log into COMMBUYS, locate the Bid, acknowledge receipt of the Bid, and scroll down to the bottom of the Bid Header page. The "Bid Q&A" button allows Bidders access to the Bid Q&A page.

2.3 Amendment Deadline

The SST reserves the right to make amendments to the Bid after initial publication. It is each Bidder's responsibility to check COMMBUYS for any amendments, addenda or modifications to this Bid, and any Bid Q&A records related to this Bid. The SST and the Commonwealth accepts no responsibility and will provide no accommodation to Bidders who submit a Quote based on an out-of-date Bid or on information received from a source other than COMMBUYS.

3 CONTRACT PERFORMANCE AND BUSINESS SPECIFICATIONS

3.1.1 Company Certifications and Affiliations

Bidders must provide authorization letters from manufacturers or dealers;

Bidders must provide copies of federal and state licenses regarding the category or categories you are bidding on.

Commodity Specifications

All pricing should reflect additional discounts for volume purchases and group purchases, if any. For example, additional discounts offered for purchasing both the weapon and duty gear should be reflected in the pricing structure.

Category 1 ***Firearms***:

List manufacturer, percentage markup over cost for each product line, and date of the price list. See "Bid Response Sheet"

Category 2 ***Ammunition***:

List manufacturer, percentage markup over cost for each product line, and date of the price list. See "Bid Response Sheet"

Category 3 ***Training***:

Training is defined as both the equipment needed to conduct successful Law Enforcement/ Correctional training and the training/ certification classes.

List all training courses offered, and the cost. Training includes, but is not limited to, armorer courses, less lethal munitions training, chemical munitions training, tactical operations courses, firearms training, weapons qualification training, and firearms instructor certifications. Please indicate if "Train the Trainer" is also available (preferred). See "Bid Response Sheet"

Category 4 Less Lethal Munitions:
Less Lethal Munitions includes Chemical Munitions and Simunitions.

List manufacturer's percentage markup over cost for each product line, and date of the price list. See "Bid Response Sheet"

Category 5 ***Miscellaneous Accessories/ Repair and Service***:
List examples and pricing for related parts, accessories, repairs, and/or services. Examples include, but are not limited to: Gun cleaning, gun parts and tools, and other related products and services not covered under statewide contracts. See "Bid Response Sheet"

3.1.2 Brand name or equal
Unless otherwise specified in this Bid, any reference to a particular trademark, trade name, patent, design, type, specifications, producer or supplier is not intended to restrict this Bid to any manufacturer or proprietor or to constitute an endorsement of any commodity or service, and the department may consider clearly identified offers of substantially equivalent commodities and services submitted in response to such reference.

3.1.3 Trade In
Bidders that agree to accept trade-ins must negotiate in good faith with Departments regarding value of the equipment to be traded in at the time of trade-in. Bidders must enclose a copy of their procurement trade-in policy in writing – scanned and uploaded.

3.1.4 Operational, electrical, environmental and other requirements
Bidders must note if any products or services offered have operational, electrical, environmental, or other requirements.

3.1.5 Performance specifications, durability, disclosures and recalls
Recalls or any information pertaining to the performance of products to include identified defects or manufacturing errors by manufacturers must be communicated by the bidder as soon as practicable. Bidder must facilitate compliance with recall, including providing upgraded replacement items and/or one for one exchange for recall compliant items.

3.1.6 Approvals and standards (UL, CE, FCC, FDA, ASTM, IEEE, NIJ)
Must meet or exceed industry standards (UL. CE, FCC, FDA, ASTM, IEEE, NIJ)

3.1.7 Warranties and guarantees
Bidders will facilitate warranties and guarantees.

3.1.8 Availability guarantees of service, service parts, accessories and supplies
Bidders will advise in good faith any lack of availability of services, parts, supplies, or product discontinuation. The contractor must obtain written approval from the Department prior to substituting products.

3.1.9 Upgrades and upgradeability
Bidders must provide all information regarding available and pending upgrades for department purchased products.

3.1.10 Operating Manuals
All operating manuals for all equipment must be enclosed with equipment purchased.

3.1.11 Product evaluations and samples

Bidder(s) awarded a contract may be required during the life of the contract to provide samples within ten (10) calendar days to the requesting Department and/or the Law Enforcement PMT for inspection of quality, construction, design and fit. Samples will be returned to bidders upon the completion of the evaluation. ***All samples will be provided at no charge to the Commonwealth***.

3.1.12 New in the box, most current version and not discontinued by the manufacturer- unless mutually agreed upon by the Commonwealth and the Bidder.

3.1.13 Open box, remanufactured and refurbished equipment & supplies provisions

Remanufactured or reconditioned is defined as products or equipment partially or fully manufactured from existing product materials where such materials are cleaned and repaired to the extent possible and reused in the new product or equipment in accordance with the original manufacturer's specifications. All unusable parts are to be removed and replaced with new or remanufactured parts, which meet OEM standards and any governing standards/ regulations. **All work must be performed by certified personnel.**

3.2 Service Specifications

3.2.1 Loaner Equipment

If the time for warranty or service repairs will exceed the specified time, the Contractor shall provide equivalent loaner equipment upon request by the customer. Loaner equipment shall be provided at no cost, including shipment to the customer's location and return of loaner equipment to the Contractor.

3.2.2 Technical Support

Describe contact, staffing, times available (e.g., 9AM-5PM EST), response time (e.g., within xx hours) and escalation procedures.
24/7 support is required for critical items.

3.2.3 Capacity plan, resources and infrastructure for this Contract

Capacity plan for meeting the contractual requirements for delivery
Local warehouse, stocking levels and order lead times
Infrastructure including facilities, trucks, equipment and offices

3.2.4 Customer forecasting (Vendor Managed Inventory or VMI)

Describe a process or service for forecasting agencies needs to maintain minimum inventory levels. Bidder must advise of any potential delays in availability, including unavailability or raw materials, price fluctuation, production or transportation delays.

3.2.5 Emergency response plans/ preparedness

In a declared state of emergency where the safety and wellbeing of Commonwealth citizens are at risk, contractors may be asked to supply the Commonwealth with the commodities and/or services under the Contract on a priority basis. The Bidder's quote should include the following:

- Indicate whether there is a written Continuity of Operations Plan (COOP) that describes how the company will continue to do business in case of an emergency.
- A list of emergency contact information including name, position/title, phone, email and cell phone.
- A list of the Bidder's building location(s) that would be available to serve the Commonwealth during an emergency.

- A description of the areas of Massachusetts that the Bidder could supply in the event of an emergency (e.g., Entire State, Specific City or Region).

*__This information will not be considered in the evaluation__

3.2.6 Removal/recycling/disposal/ destruction of old equipment and data

Bidder must agree to remove/recycle/dispose of old and/or expired equipment and data.

3.2.7 Training & training materials

Use of Contractor training facilities
Use of eligible entity facilities
Content, media, delivery and time frames
Ownership and copyright provisions of training materials designed under this Contract
Ownership and rights of copyrighted training materials
Maintenance agreements and eligibility requirements
Time & Material service and repairs
Service Level Agreements (SLAs)
Response time guarantee
Maintenance

3.2.8 Requirements for Consultant

Consultant must hold current certifications for specific function

3.2.9 Order Cancellations

The Departments may cancel orders with cause.
The Departments may choose not to renew a contract if the bidder fails to meet quoted shipping deadlines**.**

3.3 Product returns

Time constraints
Amount of credit including shipping
Return shipping costs or pickup by Contractor

3.4 Employee Requirements

Bidder must provide key employee certifications and licenses when applicable (i.e. for training, certification, equipment repair);
Successful bidders and its employees may be subject to a criminal background check.
Negative information may result in disqualification from contract execution.

3.5 Audit of Records

During the term of this Agreement and for a period of five (5) years thereafter, Department of State Police, its auditors, the Operational Services Division, the Office of the Inspector General or other authorized representatives shall be afforded access at reasonable times to Contractor's accounting records, including sales information on any system, reports or files, in order to audit all records relating to goods sold or services performed pursuant to this Agreement. If such an audit indicates that Contractor has materially overcharged Department of State Police, then the Contractor shall remit the overcharged amount and be responsible for payment of any costs associated with the audit.

The Contractor agrees to allow State and Federal auditors and state agency staff access to all the records related to this contract, and the right to copy those records, for audit, inspection and monitoring of services. Such access will be during normal business.

3.6 Should new technology become available during the contract period, the contractor will provide the new technology to the Department for evaluation/ consideration. If new technology results in

discontinued use of contracted product, then the new acceptable technology will be provided to the Department and participants at a cost that is agreeable to the Department.

3.7 **EPP promotes the purchase and use of environmentally preferable commodities and services throughout the State and local Commonwealth departments.
Products and services purchased by state agencies must be in compliance with Executive Order 515, issued October 27, 2009. Under this Executive Order, Executive Departments are required to reduce their impact on the environment and enhance public health by procuring environmentally preferable products and services (EPP's) whenever such products and services perform to satisfactory standards and represent best value, consistent with 801 CMR 21.00. In line with this directive, all contracts, whether departmental or statewide, must comply with the specifications and guidelines established by OSD and the EPP Program. EPPs are considered to be products and services that help to conserve natural resources, reduce waste, protect public health and the environment, and promote the use of clean technologies, recycled materials, and less toxic products.
This would be a desirable preference to Department of State Police. Please submit any documentation including specific data sheets on chemicals used in the process of cleaning.

3.8 Fiscal Terms/ Pricing

Compensation will be based solely on the pricing information provided by the Bidder and accepted by the Department.

All work shall be guaranteed by the awarded bidder(s).

Shipping, Freight, Delivery, Handling, Fuel Charges, etc.
The achievement of fiscal transparency requires that bidders clearly itemize and quote these charges. Final charges are subject to negotiation and will be mutually agreed upon by both parties prior to the contract start date. Agreed upon charges must be clearly itemized on invoices.

4 OTHER TERMS

4.1 Contractors Terms and Conditions

The Department is not obligated and should not complete, sign or execute any contractor or vendor contracts, invoices or other terms and conditions. It must be clearly understood that the Standard Contract Form and the Commonwealth Terms and Conditions supersede any contractor or vendor contracts, invoices or other terms and conditions. If, by chance, any said contractor or vendor contracts, invoices or other terms and conditions are signed, the signed document is immediately considered invalid.

4.2 Reporting

Contractors are responsible for compliance with all other contract reporting requirements, including, but not limited to, Supplier Diversity Program (SDP) and other contract reports, as required by this contract.

4.3 Contract Management

The "Purchaser" contact listed in the Master Blanket Purchase Order on COMMBUYS for this Contract is the Department's Contract Manager. The Department's Contract Manager is the point of contact for interested bidders during the procurement process. Bidders may contact the Contract manager if the bidder is having trouble obtaining any required attachments electronically through Commbuys. Bidders are prohibited from communicating directly with any employee of the procuring department or any member of the SST regarding this RFR except as specified in this RFR, and no other Department employee or representative is authorized to provide any information or respond to any question or inquiry regarding this RFR. The Department's Contract Monitor is the Department employee responsible for managing and administering the contract upon award. The Department's Contract Monitor will be the point of contact for the successful bidder and Contractor concerning day to day operational matters and the performance of duties of the contract.

Contract Manager:
Brian Kearnan
Brian.J.Kearnan@pol.state.ma.us

4.4 Change Notification

Changes to the Contractor's contact information, company name, legal address, payment address, tax identification number, authorized signatories, SDO-certification status, or EFT information must be promptly reported via email to the Department's Contract Manager. In some cases additional paperwork will be required to effect the change. Any change of address, including remit address, requires immediate written notification and submission of a new W-9 Form, Commonwealth Terms and Conditions and a brief letter written on contractor's letterhead stating that their address has changed "from" and "to." If written notification is not received changes cannot be done; therefore any payments will be sent to the address which is currently on file and with no late penalty to the Commonwealth.

4.5 Invoices and Payment

Itemized invoices shall be sent to the proper office by the Contractor no later than 30 days after completion of services or receipt of goods. The Contractor's invoices at a minimum shall include the following:

- Name and address of Contractor
- Telephone number and e-mail address
- Name of Department contact person and date of delivery
- Valid State Police purchase order number

All invoices shall be itemized. Itemized invoices shall include a copy of all receipts and any backup documentation. Itemized invoices shall include a complete description for each charge such as number of billable hours, the hourly rate, an explanation and description of the work performed, etc.

Invoicing and credit issues must be resolved in a timely and efficient manner. A copy of the completed, signed and detailed receipt of deliverables, which includes the department employee signature, may be attached to the invoice.

All invoices will be paid in accordance with the Office of the Comptroller's Bill Paying Policy.

Prompt Pay Discounts

Contractors are required to offer prompt pay discounts terms to the Department. Preference or additional points may be given for reasonable offers. If the Contractor offers a prompt pay discount, the discount terms must be clearly indicated on the invoices. The date the prompt payment discount term will begin is the date that the invoice is received and accepted by the Department's fiscal office or the date of work completion/order receipt, whichever is greater.

Justified Credits

Written credits will be issued to the fiscal office no later than two business days upon request. Payments will not be processed until written credits are properly received. No penalty will be issued to the Department for late payments caused by disputed invoices.

Tax Exempt

Tax shall not be charged to Executive Branch Departments. The Contractor may request a copy of the Tax Exempt form from the Department. The Department makes no guarantee that any services will be purchased from any contract resulting from this RFR. The contract resulting from this procurement creates no entitlement or guaranteed funding and payment is subject to completion and acceptance of performance by the Department.

Contractors are agreeing to these terms by submitting a Response to this RFR.

4.6 Contract Amendments

The Department reserves the right to amend this contract. The Department may negotiate changes to the original performance measures, reporting requirements or payment methodologies tied to performance at any time during the contract duration if they are consistent with the specifications of this RFR. The Department reserves the right to negotiate and execute contract amendments with the contractor(s) which the Department determines are necessary to result in the intent of this RFR, to amend the specifications for necessary requirements, or to result in a better valued contract. Negotiation would be with the successful Contractor(s) of this RFR. Amendments may include, but are not limited to, contract dollars, contract performance, increased or decreased obligations, scope of work, quantity, etc.

4.7 Contract Renewal

Prior to the expiration of the initial duration, the Department will notify Contractors of the Department's intent to renew the contract. Price changes may be requested at that time if supporting documentation of any increases is provided. Renewal rates will be negotiated at the time of the renewal offer. Contract renewal is contingent upon the Contractor's ability to perform contractual obligations.

4.8 Performance Measures

Any and all work performed through the duration of the contract must be guaranteed by the Contractor to be completed in a workmanship-like manner and according to applicable codes and industry accepted standards. Contractors will only be expected to provide services in their area(s) of expertise; that is, the business for which they receive an award. Each Contractor's performance will be evaluated on an ongoing basis and will be utilized in determining whether or not to extend the contract. Purchasers may be surveyed as to their satisfaction with the Contractor's performance under the contract. Contractor performance will also be evaluated based on the number of complaints received from Purchasers. A high number of unresolved

complaints will result in a warning to the Contractor and may lead to early termination or non-renewal of that Contractor's contract.

4.9 Insurance

The Commonwealth of Massachusetts is self-insured and does not pay for additional insurance, which means that it does not purchase separate personal and property liability insurance. The Commonwealth does not provide certificates or other proof of insurance since this is provided for in the statute M.G.L.c.258 (which has the same effect). Therefore, providing this information should obviate the need for providing further proof of insurance. Departments are prohibited from insuring Commonwealth property under M.G.L.c.29,§30 absent specific legislative authorization. This means that a department is prohibited from insuring its property or equipment from damage or loss. In addition to being prohibited from insuring its own property, a department may not insure property it does not own.

The Bidder(s) awarded contracts pursuant to this RFR **must** have sufficient insurance coverage and this insurance coverage **must** be maintained during the life of the contract. As part of the response to this RFR, Bidders **must** provide Certificates of Insurance from their insurance company which may include but is not limited to: **Commercial General Liability Insurance, Automobile Liability Insurance, Worker's Compensation Insurance, Employers Liability Insurance, Professional Liability Insurance.** Prior to beginning work pursuant to this RFR with a Subcontractor, the Contractor **must** provide the Department with certified copies of each Subcontractor's insurance policies, which **must** meet the same insurance coverage levels for Contractors as **required** under this RFR. Any policy limits set in this RFR shall not be interpreted to limit the Contractor's liability for personal or property damage in the performance of this Contract and the Contractor shall remain fully liable for any personal or property damages in the performance of this Contract.

Certificates of Insurance

Bidders must provide copies of all certificates of insurance with their response. Thereafter, Bidders must provide copies of all certificates of insurance on an annual basis.

4.10 Contract Termination for Convenience

In accordance with Section 4 of the Commonwealth Terms and Conditions, the Department of State Police may, in its sole discretion, terminate this Contract at any time without cause for its convenience ("Termination for Convenience") by giving written notice to Contractor thirty (30) calendar days prior to the effective date of termination or such other period as is mutually agreed upon in advance by the parties. If Contractor is not in default or in breach of any material term or condition of this Contract, Contractor shall be paid its reasonable, proper, and verifiable costs, including work performed and accepted up to the date of termination to the extent previous payments made by the Department of State Police to Contractor have not already done so. Such payment shall be Contractor's sole and exclusive remedy for any Termination for Convenience and, upon such payment by the Department of State Police to the Contractor, the Department of State Police shall have no further obligation to Contractor. The Department of State Police shall not be responsible for Contractors anticipatory profits or overhead costs attributable to unperformed work.

4.11 Contract Termination for Cause

In accordance with Section 4 of the Commonwealth Terms and Conditions, the Department may terminate a contract if the Contractor breaches any material term or condition or fails to perform any material obligation required by the contract.

5 EVALUATION CRITERIA

Bidder scores will be used to rank Bidders and will determine which Bidders will proceed to subsequent stages of the evaluation and/or enter into negotiations with the Commonwealth to receive a Contract award.

Mandatory requirements

Mandatory Specifications must be met in order for a Bid to be evaluated and may be used to disqualify Bidders. In addition, certain mandatory specifications have desirable components to them that may be evaluated by the SST. The SST reserves the right, in its discretion, to determine if non-compliance with a Mandatory Specification is insignificant or can be easily corrected.

Bid sections that include terms such as: “must”, “shall”, “will” and “required” are “mandatory.” Failure to meet the requirements of a mandatory specification without providing an alternate that is acceptable to the evaluators may result in the disqualification of a Bidder's proposal.

Desirable specifications

Desirable specifications will be scored according to the Evaluation Criteria.

RFR specifications prefaced with language such as: "desirable", "could," "can," "should," "preferably," "prefers," "suggested," and "requested" identify a desirable or discretionary item or factor that is considered by the Purchaser to be "desirable." The Purchaser has listed all desirable specifications which will receive points in the evaluation criteria.

Alternatives

A Quote which fails to meet any material terms or conditions of the Bid, including the submission of required attachments, may lose points or be deemed unresponsive and disqualified. Unless otherwise specified, Bidders may submit Quotes proposing alternatives which provide equivalent, better or more cost effective performance than achievable under the stated Bid specifications. These alternatives may include related commodities or services that may be available to enhance performance during the period of the Contract. The Quote should describe how any alternative achieves substantially equivalent or better performance to that of the Bid specifications.

The SST will determine if a proposed alternative method of performance achieves substantially equivalent or better performance. The goal of this Bid is to provide the best value of commodities and/or services to achieve the goals of the procurement.

Evaluation Components

The following criteria will be considered by the SST when evaluating each Quote:

CRITERIA	MAXIMUM POINTS
Price	30
Experience	15
Prompt Payment Discount	5
Business References (3)	20
Supplier Diversity Program	25
Environmentally Preferable Practices	5

6 INSTRUCTIONS FOR SUBMISSION OF RESPONSES:

Responses must be sent via the "Create Quote" functionality contained in COMMBUYS. For instructions concerning how to submit a Quote, please see **Attachment: Instructions for Vendors Responding to Bids**.

Bidders MUST also submit their response in a sealed envelope that is clearly marked with the RFR Reference number "RFR #SP21-AMMO-X86" to the following address:

Department of State Police Headquarters
470 Worcester Road
Framingham, MA 01702
Attn: Dianne Miller

Original submission must contain "wet ink" signatures. Electronic signatures are not acceptable. Submissions with electronic signatures for the originals may be disqualified as unresponsive.

Any submission which fails to meet the submission requirements of the RFR will be found non-responsive without further evaluation unless the evaluation team, at its discretion, determines that the non-compliance is insubstantial and can be corrected. In these cases, the evaluation team may allow the vendor to make minor corrections to the submission.

a. Online Questions (Bid Q&A)

Written Questions must be entered by pressing the "Bid Q&A" tab for the Bid in COMMBUYS no later than the "Online Questions Due" date and time indicated in the Estimated Procurement Calendar (above). The issuing department reserves the right not to respond to questions submitted after this date. It is the Bidder's responsibility to verify receipt of questions.

It is the responsibility of the prospective Bidder and awarded Contractor to maintain an active registration in COMMBUYS and to keep current the email address of the Bidder's contact person and prospective contract manager, if awarded a contract, and to monitor that email inbox for communications from the Purchasing Department, including requests for clarification. The Purchasing Department and the Commonwealth assume no responsibility if a prospective Bidder's/awarded Contractor's designated email address is not current, or if technical problems, including those with the prospective Bidder's/awarded Contractor's computer, network or internet service provider (ISP) cause email communications sent to/from the prospective Bidder/Awarded contractor and the Purchasing Department to be lost or rejected by any means including email or spam filtering.

Written Responses to Questions will be released on or about the "Responses to Questions Posted Online" date indicated in the Estimated Procurement Calendar (above).

(Written questions and responses will be posted on the Bid Q&A Tab for this Bid in COMMBUYS.**)**

b. Bid Amendment Deadline

The Purchasing Department reserves the right to make amendments to the Bid after initial publication. It is each Bidder's responsibility to check COMMBUYS for any amendments, addenda or modifications to this Bid, and any Bid Q&A records related to this Bid. The Purchasing Department and the Commonwealth accept no responsibility and will provide no accommodation to Bidders who

submit a Quote based on an out-of-date Bid or on information received from a source other than COMMBUYS.

c. Quotes (Bid Responses) Deadline (Bid Opening Date/Time)

See the Quotes (Bid Responses) Deadline (Bid Opening) Date and Time indicated in the Estimated Procurement Calendar (above).

d. Estimated Contract Start Date

This is the approximate start date. The actual start date will be the Contract Effective Date which is the date the Contract is executed by the parties.

6.1 Required Forms

Check if applicable ("X")	Form/Document	Notes/Instructions (If any)
☒	Commonwealth Terms & Conditions	Incorporated by reference on Standard Contract Form
☒	Massachusetts Substitute W-9 Form	Wet Ink Signature Required - upon contract award
☒	Standard Contract Form and Instructions	Wet Ink Signature Required- upon contract award
☒	Contractor Authorized Signatory Listing	Wet Ink Signature Required - upon contract award
☒	Authorization for Electronic Funds Transfer	Wet Ink Signature Required - upon contract award
☒	Supplier Diversity Program Plan	Electronic Submission with bid/quote
☒	Prompt Payment Discount Form	Electronic Submission with bid/quote
☒	Business Reference Form or Letters of Reference	Electronic Submission with bid/quote

The above attachments are available as part of the Bid record on www.commbuys.com.

7 APPENDIX 1 – REQUIRED TERMS FOR ALL RFRS

7.1 General Procurement Information

7.1.1 Access to security-sensitive information

Bidders agree to adhere to this section in the event that an eligible entity provides a Contractor with security-sensitive information which, pursuant to MGL c. 4, § 7, cls. 26(n), is generally exempt from public disclosure under the Commonwealth's public records laws and must, for public safety purposes, be safeguarded from widespread public disclosure. This security-sensitive information is in the form of blueprints, plans, policies, procedures, schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, and/or any other records relating to the security or safety of persons (pursuant to MGL c. 66A) or buildings, structures, facilities, utilities, transportation, information technology or other infrastructure located within the Commonwealth. Qualified prospective Bidders that are interested in accessing this information for the purpose of preparing a Quote must, before being allowed to access the information, sign a confidentiality agreement, thereby agreeing to:

restrict the use of these sensitive records for any other purpose than as authorized and for the purpose of putting together a bid proposal;

safeguard the information while it is in their possession (consistent with Section 6 of the Commonwealth Terms and Conditions); and

return such records and materials to the Commonwealth upon completion of the project.

7.1.2 Alterations

Bidders may not alter (manually or electronically) the Bid language or any Bid component files, except as directed in the RFR. Modifications to the body of the Bid, specifications, terms and conditions, or which change the intent of this Bid are prohibited and may disqualify a Quote.

7.1.3 Ownership of Submitted Quotes

The SST shall be under no obligation to return any Quotes or materials submitted by a Bidder in response to this Bid. All materials submitted by Bidders become the property of the Commonwealth of Massachusetts and will not be returned to the Bidder. The Commonwealth reserves the right to use any ideas, concepts, or configurations that are presented in a Bidder's Quote, whether or not the Quote is selected for Contract award.

Quotes stored on COMMBUYS in the encrypted lock-box are the file of record. Bidders retain access to a read-only copy of this submission via COMMBUYS, as long as their account is active. Bidders may also retain a traditional paper copy or electronic copy on a separate computer or network drive or separate media, such as CD or DVD, as a backup.

7.1.4 Prohibitions

Bidders are prohibited from communicating directly with any employee of the procuring Department or any member of the SST regarding this RFR except as specified in this RFR, and no other individual Commonwealth employee or representative is authorized to provide any information or respond to any question or inquiry concerning this RFR. Bidders may contact the contact person using the contact information provided in the Header Information this Bid in the event that this RFR is incomplete or information is missing. Bidders experiencing technical problems accessing information or attachments stored on COMMBUYS should contact the COMMBUYS Helpdesk (see the document cover page for contact information).

In addition to the certifications found in the Commonwealth's Standard Contract Form, by submitting a Quote, the Bidder certifies that the Quote has been arrived at independently and has been submitted without any communication, collaboration, or without any agreement, understanding or planned common course or action with, any other Bidder of the commodities and/or services described in the RFR.

7.2 Terms and Requirements Pertaining to Awarded Contracts

7.2.1 Commonwealth Tax Exemption

Invoices or invoices submitted to Massachusetts government entities must not include sales tax.

7.2.2 Contractor's Contact Information

It is the Contractor's responsibility to keep the Contractor's Contract Manager information current. If this information changes, the Contractor must notify the Contract Manager by email immediately, using the address located in the Header Information of the Purchase Order or Master Blanket Purchase Order on COMMBUYS.

The Commonwealth assumes no responsibility if a Contractor's designated email address is not current, or if technical problems, including those with the Contractor's computer, network or internet service provider (ISP), cause e-mail communications between the Bidder and the SST to be lost or rejected by any means including email or spam filtering.

7.2.3 Publicity

Any Contractor awarded a contract under this Bid is prohibited from selling or distributing any information collected or derived from the Contract, including lists of participating Eligible Entities, Commonwealth employee names, telephone numbers or addresses, or any other information except as specifically authorized by the SST.

8 APPENDIX 2 - RFR - REQUIRED SPECIFICATIONS

In general, most of the required contractual stipulations are referenced in the *Standard Contract Form and Instructions* and the *Commonwealth Terms and Conditions* (either version). However, the following RFR provisions must appear in all Commonwealth competitive procurements conducted under 801 CMR 21.00:

The terms of *801 CMR 21.00: Procurement of Commodities and Services* (and *808 CMR 1.00: Compliance, Reporting and Auditing for Human and Social Services*, if applicable) are incorporated by reference into this RFR. Words used in this RFR shall have the meanings defined in 801 CMR 21.00 (and 808 CMR 1.00, if applicable). Additional definitions may also be identified in this RFR. Other terms not defined elsewhere in this document may be defined in OSD's Glossary of Terms. Unless otherwise specified in this RFR, all communications, responses, and documentation must be in English, all measurements must be provided in feet, inches, and pounds and all cost proposals or figures in U.S. currency. All responses must be submitted in accordance with the specific terms of this RFR.

Items with the text, "☞ *Required for POS Only"* specify a requirement for Purchase of Service (POS) human and social services procured under *801 CMR 21.00, Procurement of Commodities or Services, Including Human and Social Services* and *808 CMR 1.00, Compliance, Reporting and Auditing for Human and Social Service.*

COMMBUYS Market Center. COMMBUYS is the official source of information for this Bid and is publicly accessible at no charge at www.commbuys.com. Information contained in this document and in COMMBUYS, including file attachments, and information contained in the related Bid Questions and Answers (Q&A), are all components of the Bid, as referenced in COMMBUYS, and are incorporated into the Bid and any resulting contract.

Bidders are solely responsible for obtaining all information distributed for this Bid via COMMBUYS. Bid Q&A supports Bidder submission of written questions associated with a Bid and publication of official answers.

It is each Bidder's responsibility to check COMMBUYS for:

- Any amendments, addenda or modifications to this Bid, and
- Any Bid Q&A records related to this Bid.

The Commonwealth accepts no responsibility and will provide no accommodation to Bidders who submit a Quote based on an out-of-date Bid or on information received from a source other than COMMBUYS.

COMMBUYS Subscription. Bidders may elect to obtain a free COMMBUYS Seller subscription which provides value-added features, including automated email notification associated with postings and modifications to COMMBUYS records. However, in order to respond to a Bid, Bidders must register and maintain an active COMMBUYS Seller subscription account.

All Bidders submitting a Quote (previously referred to as Response) in response to this Bid (previously referred to as Solicitation) agree that, if awarded a contract: (1) they will maintain an active seller account in COMMBUYS; (2) they will, when directed to do so by the procuring entity, activate and maintain a COMMBUYS-enabled catalog using Commonwealth Commodity Codes; (3) they will comply with all requests by the procuring entity to utilize COMMBUYS for the purposes of conducting all aspects of purchasing and invoicing with the Commonwealth, as added functionality for the COMMBUYS system is activated; (4) Bidder understands and acknowledges that all references to the Comm-PASS website or related requirements throughout this RFR, shall be superseded by comparable requirements pertaining to the COMMBUYS website; and (6) in the event the Commonwealth adopts an alternate market center system, successful Bidders will be required to utilize such system, as directed by the procuring entity. Commonwealth Commodity Codes are based on the United Nations Standard Products and Services Code (UNSPSC).

The COMMBUYS system introduces new terminology, which bidders must be familiar with in order to conduct business with the Commonwealth. To view this terminology and to learn more about the COMMBUYS system, please visit the COMMBUYS Resource Center.

Multiple Quotes. Bidders may not submit Multiple Quotes in response to a Bid unless the RFR authorizes them to do so. If a Bidder submits multiple quotes in response to an RFR that does not authorize multiple responses, only the latest dated quote submitted prior to the bid opening date will be evaluated.

Quote Content. Bid specifications for delivery, shipping, billing and payment will prevail over any proposed Bidder terms entered as part of the Quote, unless otherwise specified in the Bid.

Supplier Diversity Program (SDP). Massachusetts Executive Order 565 reaffirmed and expanded the Commonwealth's policy to promote the award of state contracts in a manner that develops and strengthens certified Minority Business Enterprises (MBEs), Women Business Enterprises (WBEs), Minority and Women Nonprofit Organizations (M/WNPOs), Veteran Business Enterprises (VBEs), Service-Disabled Veteran-Owned Business Enterprises (SDVOBEs), Disability-Owned Business Enterprises (DOBEs), and Lesbian, Gay, Bisexual and Transgender Business Enterprises (LGBTBEs).

Partnerships with certified diverse businesses: All bidders are **required** to make a significant financial commitment to partner with certified M/WBEs, M/WNPOs, VBEs, SDVOBEs, DOBEs and/or LGBTBEs certified or verified by the Supplier Diversity Office (SDO). Bidders must identify a commitment in the form of a specific percentage of sales made under the resulting contract that will be spent with an SDP Partner(s) on a Massachusetts fiscal year basis, using the SDP Plan Form. This percentage commitment will extend for the life of any resulting contract.

This requirement extends to all bidders regardless of their certification status, and no bidder will be awarded a Contract unless and until the above requirement is met. Bidders may not list themselves or affiliates as SDP Partners. In order to ensure compliance with this section and encourage bidder participation, SDP Plans will be evaluated at 25% or more of the total evaluation score for all for Large Procurements (those with a total annual value of greater than $250,000). SDP Plan submission is encouraged but not required for Small Procurements (those with a total annual value equal to or less than $250,000).

Once an SDP commitment is approved, the agency will monitor the Contractor's performance, and use the Contractor's reported expenditures with M/WBEs, M/WNPOs, VBEs, SDVOBEs, and LGBTBEs to fulfill their own SDP expenditure benchmarks. The Commonwealth reserves the right to contact SDP Partners at any time to request that they attest to the amounts reported to have been paid to them by the Contractor.

SDP Forms: Unless otherwise specified in the RFR, the following SDP forms are required to be submitted by the deadlines noted below in order to meet the mandatory participation requirements of the SDP:

SDP Plan Form #/Name	Submitted By	When Submitted
SDP Plan Form – SDP Plan Commitment and Partner(s)	All Bidders	With Bid Response
SDP Plan Spending Report	Contractors	Within 45 days after end of quarter

In addition to the requirements above, all bidders must follow the requirements set forth in the Supplier Diversity Program (SDP) Plan Section of the RFR. During the life of the contract, the Commonwealth reserves the right to expand the range of certified business categories available for SDP partnerships to all those mentioned above and/or request reports on the Contractors' spending with such certified business categories.

Supplier Diversity Program (SDP) Resources: Bidders may refer to the SDP Resources for Vendors and Contractors webpage for additional program information, training and compliance resources.

Best Value Selection and Negotiation. The Strategic Sourcing Team or SST (formerly referred to as Procurement Management Team or PMT) may select the response(s) which demonstrates the best value overall, including proposed alternatives that will achieve the procurement goals of the department. The SST and a selected bidder, or a contractor, may negotiate a change in any element of contract performance or cost identified in the original RFR or the selected bidder's or contractor's response which results in lower costs or a more cost effective or better value than was presented in the selected bidder's or contractor's original response.

Bidder Communication. Bidders are prohibited from communicating directly with any employee of the procuring department or any member of the SST regarding this RFR except as specified in this RFR, and no other individual Commonwealth employee or representative is authorized to provide any information or respond to any question or inquiry concerning this RFR. Bidders may contact the contact person for this RFR in the event this RFR is incomplete or the bidder is having trouble obtaining any required attachments electronically through COMMBUYS.

Contract Expansion. If additional funds become available during the contract duration period, the department reserves the right to increase the maximum obligation to some or all contracts executed as a result of this RFR or to execute contracts with contractors not funded in the initial selection process, subject to available funding, satisfactory contract performance and service or commodity need.

Costs. Costs which are not specifically identified in the bidder's response, and accepted by a department as part of a contract, will not be compensated under any contract awarded pursuant to this RFR. The Commonwealth will not be responsible for any costs or expenses incurred by bidders responding to this RFR.

Electronic Communication/Update of Bidder's/Contractor's Contact Information. It is the responsibility of the prospective bidder and awarded contractor to keep current on COMMBUYS the email address of the bidder's contact person and prospective contract manager, if awarded a contract, and to monitor that email inbox for communications from the SST, including requests for clarification. The SST and the Commonwealth assume no responsibility if a prospective bidder's/awarded contractor's designated email address is not current, or if technical problems, including those with the prospective bidder's/awarded contractor's computer, network or internet service provider (ISP) cause email communications sent to/from the prospective bidder/awarded contractor and the SST to be lost or rejected by any means including email or spam filtering.

Electronic Funds Transfer (EFT). All bidders responding to this RFR must agree to participate in the Commonwealth Electronic Funds Transfer (EFT) program for receiving payments, unless the bidder can provide compelling proof that it would be unduly burdensome. EFT is a benefit to both contractors and the Commonwealth because it ensures fast, safe and reliable payment directly to contractors and saves both parties the cost of processing checks. Contractors are able to track and verify payments made electronically through the Comptroller's Vendor Web system. A link to the EFT application can be found on the OSD Forms page (www.mass.gov/osd). Additional information about EFT is available on the VendorWeb site (www mass.gov/osc). Click on MASSfinance.

Successful bidders, upon notification of contract award, will be required to enroll in EFT as a contract requirement by completing and submitting the *Authorization for Electronic Funds Payment Form* to this department for review, approval and forwarding to the Office of the Comptroller. If the bidder is already enrolled in the program, it may so indicate in its response. Because the *Authorization for Electronic Funds Payment Form* contains banking information, this form, and all information contained on this form, shall not be considered a public record and shall not be subject to public disclosure through a public records request.

The requirement to use EFT may be waived by the SST on a case-by-case basis if participation in the program would be unduly burdensome on the bidder. If a bidder is claiming that this requirement is a hardship or unduly burdensome, the specific reason must be documented in its response. The SST will consider such requests on a case-by-case basis and communicate the findings with the bidder.

Environmental Response Submission Compliance. In the event that paper submissions are required and in an effort to promote greater use of recycled and environmentally preferable products and minimize waste, all required paper responses that are submitted should comply with the following guidelines:

- All copies should be printed double sided.
- All submittals and copies should be printed on recycled paper with a minimum post-consumer content of 30% or on tree-free paper (i.e. paper made from raw materials other than trees, such as kenaf). To document the use of such paper, a photocopy of the ream cover/wrapper should be included with the response.
- Unless absolutely necessary, all responses and copies should minimize or eliminate use of non-recyclable or non re-usable materials such as plastic report covers, plastic dividers, vinyl sleeves and GBC binding. Three ringed binders, glued materials, paper clips and staples are acceptable.
- Bidders should submit materials in a format which allows for easy removal and recycling of paper materials.
- Bidders are encouraged to use other products which contain recycled content in their response documents. Such products may include, but are not limited to, folders, binders, paper clips, diskettes, envelopes, boxes, etc. Where appropriate, bidders should note which products in their responses are made with recycled materials.
- Unnecessary samples, attachments or documents not specifically asked for should not be submitted.

Executive Order 509, *Establishing Nutrition Standards for Food Purchased and Served by State Agencies*. Food purchased and served by state agencies must be in compliance with Executive Order 509, issued in January 2009. Under this Executive Order, all contracts resulting from procurements posted after July 1, 2009 that involve the purchase and provision of food must comply with nutrition guidelines established by the Department of Public Health (DPH). The nutrition guidelines are available at the Department's website: Executive Order # 509 Guidance.

HIPAA: Business Associate Contractual Obligations. Bidders are notified that any department meeting the definition of a Covered Entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will include in the RFR and resulting contract sufficient language establishing the successful bidder's contractual obligations, if any, that the department will require in order for the department to comply with HIPAA and the privacy and security regulations promulgated thereunder (45 CFR Parts 160, 162, and 164) (the Privacy and Security Rules). For example, if the department determines that the successful bidder is a business associate performing functions or activities involving protected health information, as such terms are used in the Privacy and Security Rules, then the department will include in the RFR and resulting contract a sufficient description of business associate's contractual obligations regarding the privacy and security of the protected health information, as listed in 45 CFR 164.314 and 164.504 (e), including, but not limited to, the bidder's obligation to: implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the protected health information (in whatever form it is maintained or used, including verbal communications); provide individuals access to their records; and strictly limit use and disclosure of the protected health information for only those purposes approved by the department. Further, the department reserves the right to add any requirement during the course of the contract that it determines it must include in the contract in order for the department to comply with the Privacy and Security Rules. Please see other sections of the RFR for any further HIPAA details, if applicable.

Minimum Quote (Bid Response) Duration. Bidders Quotes made in response to this Bid must remain in effect for at least 90 days from the date of quote submission.

Prompt Payment Discounts (PPD). All bidders responding to this procurement must agree to offer discounts through participation in the Commonwealth Prompt Payment Discount (PPD) initiative for receiving early and/or on-time payments, unless the bidder can provide compelling proof that it would be unduly burdensome. PPD benefits both contractors and the Commonwealth. Contractors benefit by increased, usable cash flow as a result of fast and efficient payments for commodities or services rendered. Participation in the Electronic Funds Transfer initiative further maximizes the benefits with payments directed to designated accounts, thus eliminating the impact of check clearance policies and traditional mail lead time or delays. The Commonwealth benefits because contractors reduce the cost of products and services through the applied discount. Payments that are processed electronically can be tracked and verified through the Comptroller's Vendor Web system. The PPD form can be found as an attachment for this Bid on COMMBUYS.

Bidders must submit agreeable terms for Prompt Payment Discount using the PPD form within their proposal, unless otherwise specified by the SST. The SST will review, negotiate or reject the offering as deemed in the best interest of the Commonwealth.

The requirement to use PPD offerings may be waived by the SST on a case-by-case basis if participation in the program would be unduly burdensome on the bidder. If a bidder is claiming that this requirement is a hardship or unduly burdensome, the specific reason must be documented in or attached to the PPD form.

Public Records. All responses and information submitted in response to this RFR are subject to the Massachusetts Public Records Law, M.G.L., c. 66, s. 10, and to c. 4, s. 7, ss. 26. Any statements in submitted responses that are inconsistent with these statutes shall be disregarded.

Reasonable Accommodation. Bidders with disabilities or hardships that seek reasonable accommodation, which may include the receipt of RFR information in an alternative format, must communicate such requests in writing to the contact person. Requests for accommodation will be addressed on a case by case basis. A bidder requesting accommodation must submit a written statement which describes the bidder's disability and the requested accommodation to the contact person for the RFR. The SST reserves the right to reject unreasonable requests.

Restriction on the Use of the Commonwealth Seal. Bidders and contractors are not allowed to display the Commonwealth of Massachusetts Seal in their bid package or subsequent marketing materials if they are awarded a contract because use of the coat of arms and the Great Seal of the Commonwealth for advertising or commercial purposes is prohibited by law.

Subcontracting Policies. Prior approval of the department is required for any subcontracted service of the contract. Contractors are responsible for the satisfactory performance and adequate oversight of its subcontractors. Human and social service subcontractors are also required to meet the same state and federal financial and program reporting requirements and are held to the same reimbursable cost standards as contractors.

9 APPENDIX 3 INSTRUCTIONS FOR EXECUTION AND SUBMISSION OF COMMONWEALTH STANDARD FORMS

The purpose of this appendix is to provide guidance to Bidders on the Commonwealth Standard forms to be submitted (in addition to the other forms and documents required) and how they must be executed and submitted. Please note that these instructions are meant to supplement the Instructions found on each of these forms. It is advisable to print this document first so that it may be referenced when filling out these forms.

Some of the forms listed below can be electronically signed by the Bidder, see Electronic Signatures. However, online Bidders must, if notified of Contract award, submit the following four (4) forms on paper with original ink signatures unless otherwise specified below, within the timeframe referenced in the RFR section entitled Ink Signatures: the Commonwealth Standard Contract Form, the Commonwealth Terms and Conditions, the Request for Taxpayer Identification Number and Certification (Mass. Substitute W9 Form) and the Contractor Authorized Signatory Listing.

9.1 Commonwealth Standard Contract Form

Sign electronically as described above; **if notified of Contract award**, complete as directed below and submit on paper with original ink signature and date.

By executing this document or signing it electronically, the Bidder certifies, under the pains and penalties of perjury, that it has submitted a Response to this RFR that is the Bidder's Offer as evidenced by the execution of its authorized signatory, and that the Bidder's Response may be subject to negotiation by the SST. Also, the terms of the RFR, the Bidder's Response and any negotiated terms shall be deemed accepted by the Operational Services Division and included as part of the Contract upon execution of this document by the State Purchasing Agent or his designee.

If the Bidder does not have a Vendor Code beginning with "VC," or does not know what their Vendor Code is, the Bidder should leave the Vendor Code field blank. The Bidder should NOT enter a Vendor Code assigned prior to May 2004, as new Vendor Codes have been assigned to all companies since that time.

Signature and date MUST be handwritten in ink, and the signature must be that of one of the people authorized to execute contracts on behalf of the Contractor on the Contractor Authorized Signatory Listing (See below).

9.2 Commonwealth Terms and Conditions

The Standard Contract form incorporates the Commonwealth Terms & Conditions by reference. ***This means that signing the Standard Contract Form also signifies acceptance of the applicable terms and conditions of this document, and there is no need to separately sign the Commonwealth Terms & Conditions.*** This document must be unconditionally accepted by one of the authorized signatories (see Contractor Authorized Signatory Listing, below), and accepted without alteration. If the provisions in this document are not acceptable in their entirety without modification, the entire Proposal offered in the response to this Solicitation may be deemed non-responsive. The awarded Contractor certifies compliance with the Commonwealth Terms & Conditions as certified by its authorized signatory in the Standard Contract Form.

9.3 Request for Taxpayer Identification Number and Certification (Mass. Substitute W9 Form)

Sign electronically as described above; **if notified of Contract award**, complete as directed below and submit on paper with original ink signature and date, or submit a copy of a previously executed, up-to-date copy of the form as directed below.

If a Bidder has already submitted a Request for Taxpayer Identification and Certification Number (Mass. Substitute W9 Form) and has received a valid Massachusetts Vendor Code, an original W-9 form is not required. A copy of the form as filed may be included in place of an original. If the Bidder's name, address or Tax ID Number have changed since the Mass. Substitute W9 Form was executed, a new Mass. Substitute W9 Form is required. The information on this form will be used to record the Bidder's legal address and where payments under a State Contract will be

sent. The company's correct legal name and legal address must appear on this form, and must be identical to the legal name and legal address on the Commonwealth Terms and Conditions. Please do not use the U.S Treasury's version of the W9 Form.

9.4 Contractor Authorized Signatory Listing

Sign electronically as described above; **if notified of Contract award**, complete as directed below and submit on paper with original ink signature and date.

In the table entitled "Authorized Signatory Name" and "Title," type the names and titles of those individuals authorized to execute contracts and other legally binding documents on behalf of the Bidder. Bidders are advised to keep this list as small as possible, as Contractors will be required to notify the Procurement Manager of any changes. If the person signing in the signature block on the bottom of the first page of this form will also serve as an "Authorized Signatory," that person's name must be included in the typed table.

With regard to the next paragraph, which begins "I certify that I am the President, Chief Executive Officer, Chief Fiscal Officer, Corporate Clerk or Legal Counsel for the Contractor…," if your organization does not have these titles, cross them out and handwrite the appropriate title above the paragraph.

The signature and date should be handwritten in ink. Title, telephone, fax and eMail should be typed or handwritten legibly.

The second page of the form (entitled "Proof of Authentication of Signature") states that the page is optional. However, the "optional" aspect of the form is that Commonwealth Departments are not required to use it. In the case of Statewide Contracts, this page is REQUIRED, not optional. The person signing this page must be the same person signing the Standard Contract Form, the Commonwealth Terms and Conditions, and the RFR Checklist.

Please note that in two places where the form says "in the presence of a notary," this should be interpreted to mean "in the presence of a notary or corporate clerk/secretary." Either a notary or corporate clerk/secretary can authenticate the form; only one is required.

Organizations whose corporate clerks/secretaries authenticate this form are not required to obtain a Corporate Seal to complete this document.

9.5 Supplier Diversity Program Plan

NOTE: SDP is REQUIRED for procurements over $250,000 (total annual earnings).

Download this form and complete as directed below; include with online submission. Ink signature is not required.

The specific Supplier Diversity Program (SDP) requirements for this procurement can be found earlier in this document. Bidders are required to state a specific percentage of contract revenues that will represent the SDP commitment for the entire contract period, including any renewals.

9.6 Additional Environmentally Preferable Products / Practices

In line with the Commonwealth's efforts to promote products and practices which reduce our impact on the environment and human health, Bidders are encouraged to provide information regarding their environmentally preferable/sustainable business practices as they relate to this Contract wherever possible. Bidders must complete this form and submit it with their RFR Response.

9.7 Prompt Payment Discount Form

Download this form and complete as directed below; include with online submission. Ink signature is not required.

Pursuant to the Prompt Payment Discount terms set forth in the RFR Required Specifications for Contracts and on the Prompt Payment Discount Form itself, all Bidders must execute this form. After entering the "Bidder Name" and "Date of Offer for Prompt/Early Payment Discount", the

Bidder must identify the prompt payment discount(s) terms by indicating the "Percentage Discount off of the Proposed Pricing" and the "Turn-around-time for Payments." In the event of a hardship that prevents the Bidder from offering a prompt payment discount, the Bidder must document this fact and provide supporting information. If awarded a contract, the final negotiated prompt payment discounts should be reflected on the Commonwealth Standard Contract Form.

9.8 Business Reference Form

Download this form and complete as directed below; include with online submission. Ink signature is not required.

Bidders must provide all requested information on this form for three (3) business references. In completing this form, note that the "Bidder" is the name of the company submitting a Quote in response to this RFR and the "RFR Name/Title" and the "Agency Document Number" can be found on the cover of the RFR document and in the Short Description field in the Header Information of the Bid record in COMMBUYS. Also, please note that: "Reference Name" is the name of the organization (if not applicable, then name of the individual) that is providing the reference; "Contact" is the name of the individual inside the organization that will provide the reference; and the "Address," "Phone #" and "Fax/Internet Address" are those of the "Contact" so that the SST may be able to reach them.

10 APPENDIX 4 - GLOSSARY

In addition to the definitions found in 801 CMR 21.00, which apply to all procurements for goods and services, the definitions found below apply to this Solicitation. Those definitions below designated with an asterisk ("*") are quoted directly from 801 CMR 21.00 and are included below for quick reference purposes.

Agency – See Department

Bid – While a bid may generally refer to an offer or response submitted in response to a Solicitation or Request for Response (RFR), in COMMBUYS, a "bid" refers to the solicitation, RFR or procurement.

Bidder * - An individual or organization proposing to enter into a Contract to provide a Commodity or Service, or both, to or for a Department or the State.

Commonwealth Contract Manager – See Strategic Sourcing Services Lead

Contract * - A legally enforceable agreement between a Contractor and a Department. ANF, OSD and CTR shall jointly issue Commonwealth Terms and Conditions, a Standard Contract Form and other forms or documentation that Departments shall use to document the Procurement of Commodities or Services, or both. COMMBUYS refers to Contract records as "Purchase Orders" or "Blanket Purchase Orders."

Contractor * - An individual or organization which enters into a Contract with a Department or the State to provide Commodities or Services, or both.

Contractor Contract Manager – The individual designated by the Contractor to interface with the Commonwealth.

Department - For the purposes of this Solicitation, the terms "Department," "Eligible Entity," "Agency," "Commonwealth Agency," and "Contracting Department" include all entities listed in the Eligible Entities section of this RFR. COMMBUYS refers to such entities as "Organizations."

Eligible Entity – See Department

Environmentally Preferable Product (EPP) - A product or service that has a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. Such products or services may include, but are not limited to, those which contain recycled content, minimize waste, conserve energy or water, and reduce the amount of toxic materials either disposed of or consumed.

Evaluation – The process, conducted by the Strategic Sourcing Team, of reviewing, scoring and ranking the submitted Quotes related to this Bid.

FY – See Fiscal Year

F**iscal Year** - The year beginning with July first and ending with the following June thirtieth as defined in M.G.L. Chapter 4, Section 7. This may also be referred to as the "State Fiscal Year."

Organization – See Department

Procurement Team Leader (PTL) – See Strategic Sourcing Services Lead

PTL – See Procurement Team Leader

Purchasing Entity – Same as "Eligible Entity."

Quote or Response - generally refers to the offer submitted in response to a Bid or Request for Response (RFR).

Request for Response (RFR) * – The mechanism used to communicate Procurement specifications and to request Quotes from potential Bidders. An RFR may also be referred to as a "Bid" or "Solicitation."

Response – The Bidder's complete submission (or "Quote" as referenced in COMMBUYS) in response to a Solicitation, in other words, a "Bid" or "Proposal."

Solicitation – See Request for Response (RFR)

SST – See Strategic Sourcing Team

SSSL – See Strategic Sourcing Services Lead

Strategic Sourcing Team (SST) – Representatives from various eligible entities and interested stakeholders that design procurements, develop specifications, conduct Solicitations, evaluate responses to Bids and award Statewide or Department Contracts. The SST also monitors Contractor performance through performance measures and the level of customer satisfaction throughout the life of the Contract. In some agencies, SSTs are referred to as "Procurement Management Teams (PMT)."

Strategic Sourcing Services Lead (SSSL) – Individual designated by the procuring Department to lead the Strategic Sourcing Team and the solicitation and resulting contract. In some agencies SSSLs are referred to as "Procurement Team Leads (PTL)." COMMBUYS Refers to the SSSL in the Header Information section of a Bid as the "Purchaser."

COMMONWEALTH OF MASSACHUSETTS ~ STANDARD CONTRACT FORM

This form is jointly issued and published by the Office of the Comptroller (CTR), the Executive Office for Administration and Finance (ANF), and the Operational Services Division (OSD) as the default contract for all Commonwealth Departments when another form is not prescribed by regulation or policy. The Commonwealth deems void any changes made on or by attachment (in the form of addendum, engagement letters, contract forms or invoice terms) to the terms in this published form or to the Standard Contract Form Instructions and Contractor Certifications, the Commonwealth Terms and Conditions for Human and Social Services or the Commonwealth IT Terms and Conditions which are incorporated by reference herein. Additional non-conflicting terms may be added by Attachment. Contractors are required to access published forms at CTR Forms: https://www.mass.gov/lists/osd-forms. Forms are also posted at OSD Forms: https://www.macomptroller.org/forms.

CONTRACTOR LEGAL NAME: BainCor, Inc. (and d/b/a):	**COMMONWEALTH DEPARTMENT NAME:** Department of State Police **MMARS Department Code:** POL
Legal Address: (W-9, W-4): 763 South St, Holbrook, MA 02343	**Business Mailing Address:** 470 Worcester Rd, Framingham, MA 01702
Contract Manager: Wayne Bainter — **Phone:** 339-987-5525	**Billing Address (if different):**
E-Mail: wbainter@baincor.com — **Fax:**	**Contract Manager:** Brian Kearnan — **Phone:** 508-820-2127
Contractor Vendor Code: VC0000506451	**E-Mail:** Brian.J.Kearnan@pol.state.ma.us — **Fax:**
Vendor Code Address ID (e.g. "AD001"): AD___. (Note: The Address ID must be set up for EFT payments.)	**MMARS Doc ID(s):**
	RFR/Procurement or Other ID Number: BD-20-1030-0P100-0P070-49476

X NEW CONTRACT

PROCUREMENT OR EXCEPTION TYPE: (Check one option only)

- __ **Statewide Contract** (OSD or an OSD-designated Department)
- __ **Collective Purchase** (Attach OSD approval, scope, budget)
- X **Department Procurement** (includes all Grants - 815 CMR 2.00) (Solicitation Notice or RFR, and Response or other procurement supporting documentation)
- __ **Emergency Contract** (Attach justification for emergency, scope, budget)
- __ **Contract Employee** (Attach Employment Status Form, scope, budget)
- __ **Other Procurement Exception** (Attach authorizing language, legislation with specific exemption or earmark, and exception justification, scope and budget)

___ CONTRACT AMENDMENT

Enter **Current Contract End Date *Prior*** to Amendment: _____, 20___.

Enter **Amendment Amount:** $ _____. (or "no change")

AMENDMENT TYPE: (Check one option only. Attach details of amendment changes.)

- __ **Amendment to Date, Scope or Budget** (Attach updated scope and budget)
- __ **Interim Contract** (Attach justification for Interim Contract and updated scope/budget)
- __ **Contract Employee** (Attach any updates to scope or budget)
- __ **Other Procurement Exception** (Attach authorizing language/justification and updated scope and budget)

The Standard Contract Form Instructions and Contractor Certifications and the following Commonwealth Terms and Conditions document are incorporated by reference into this Contract and are legally binding: (Check ONE option): X Commonwealth Terms and Conditions __ Commonwealth Terms and Conditions For Human and Social Services __ Commonwealth IT Terms and Conditions

COMPENSATION: (Check ONE option): The Department certifies that payments for authorized performance accepted in accordance with the terms of this Contract will be supported in the state accounting system by sufficient appropriations or other non-appropriated funds, subject to intercept for Commonwealth owed debts under 815 CMR 9.00.

X **Rate Contract.** (No Maximum Obligation) Attach details of all rates, units, calculations, conditions or terms and any changes if rates or terms are being amended.)

__ **Maximum Obligation Contract.** Enter total maximum obligation for total duration of this contract (or *new* total if Contract is being amended). $ _____.

PROMPT PAYMENT DISCOUNTS (PPD): Commonwealth payments are issued through EFT 45 days from invoice receipt. Contractors requesting accelerated payments must identify a PPD as follows: Payment issued within 10 days __% PPD; Payment issued within 15 days __% PPD; Payment issued within 20 days __% PPD; Payment issued within 30 days __% PPD. If PPD percentages are left blank, identify reason: __agree to standard 45 day cycle __ statutory/legal or Ready Payments (M.G.L. c. 29, § 23A); __ only initial payment (subsequent payments scheduled to support standard EFT 45 day payment cycle. See Prompt Pay Discounts Policy.)

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE or REASON FOR AMENDMENT: (Enter the Contract title, purpose, fiscal year(s) and a detailed description of the scope of performance or what is being amended for a Contract Amendment. Attach all supporting documentation and justifications.) **Contract with MSP per multiple user option of MassDOT RFR and Commbuys bid # BD-20-1030-0P100-0P070-49476. See attached documentation.**

ANTICIPATED START DATE: (Complete ONE option only) The Department and Contractor certify for this Contract, or Contract Amendment, that Contract obligations:

X 1. may be incurred as of the Effective Date (latest signature date below) and no obligations have been incurred prior to the Effective Date.

__ 2. may be incurred as of _____, 20___, a date LATER than the Effective Date below and no obligations have been incurred prior to the Effective Date.

__ 3. were incurred as of _____, 20___, a date PRIOR to the Effective Date below, and the parties agree that payments for any obligations incurred prior to the Effective Date are authorized to be made either as settlement payments or as authorized reimbursement payments, and that the details and circumstances of all obligations under this Contract are attached and incorporated into this Contract. Acceptance of payments forever releases the Commonwealth from further claims related to these obligations.

CONTRACT END DATE: Contract performance shall terminate as of June 30, 2025, with no new obligations being incurred after this date unless the Contract is properly amended, provided that the terms of this Contract and performance expectations and obligations shall survive its termination for the purpose of resolving any claim or dispute, for completing any negotiated terms and warranties, to allow any close out or transition performance, reporting, invoicing or final payments, or during any lapse between amendments.

CERTIFICATIONS: Notwithstanding verbal or other representations by the parties, the **"Effective Date"** of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified above, subject to any required approvals. The Contractor certifies that they have accessed and reviewed all documents incorporated by reference as electronically published and the Contractor makes all certifications required under the Standard Contract Form Instructions and Contractor Certifications under the pains and penalties of perjury, and further agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein according to the following hierarchy of document precedence, the applicable Commonwealth Terms and Conditions, this Standard Contract Form, the Standard Contract Form Instructions and Contractor Certifications, the Request for Response (RFR) or other solicitation, the Contractor's Response (excluding any language stricken by a Department as unacceptable, and additional negotiated terms, provided that additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.

AUTHORIZING SIGNATURE FOR THE CONTRACTOR:

X: Wayne Bainter, **Date:** 1-18-22

(Signature and Date Must Be Captured At Time of Signature)

Print Name: WAYNE BAINTER

Print Title: PRESIDENT

AUTHORIZING SIGNATURE FOR THE COMMONWEALTH:

X: Michelle Small, **Date:** 1-19-22

(Signature and Date Must Be Captured At Time of Signature)

Print Name: Michelle Small

Print Title: Chief Administrative Officer

Issued May 2004

Massachusetts Department of Transportation
CONTRACTOR AUTHORIZED SIGNATORY LISTING

CONTRACTOR LEGAL NAME: BainCor, INC.
CONTRACTOR VENDOR/CUSTOMER CODE: VC 0000506451

INSTRUCTIONS: Any Contractor (other than a sole-proprietor or an individual contractor) must provide a listing of individuals who are authorized as legal representatives of the Contractor who can sign contracts and other legally binding documents related to the contract on the Contractor's behalf. In addition to this listing, any state department may require additional proof of authority to sign contracts on behalf of the Contractor, or proof of authenticity of signature (a notarized signature that the Department can use to verify that the signature and date that appear on the Contract or other legal document was actually made by the Contractor's authorized signatory, and not by a representative, designee or other individual.)

NOTICE: ***Acceptance of any payment under a Contract or Grant shall operate as a waiver of any defense by the Contractor challenging the existence of a valid Contract due to an alleged lack of actual authority to execute the document by the signatory.***

For privacy purposes **DO NOT ATTACH** any documentation containing personal information, such as bank account numbers, social security numbers, driver's licenses, home addresses, social security cards or any other personally identifiable information that you do not want released as part of a public record. The Commonwealth reserves the right to publish the names and titles of authorized signatories of contractors.

AUTHORIZED SIGNATORY NAME	TITLE
Wayne Bainter	President
John Cordeiro	Vice President

I certify that I am the President, Chief Executive Officer, Chief Fiscal Officer, Corporate Clerk or Legal Counsel for the Contractor and as an authorized officer of the Contractor I certify that the names of the individuals identified on this listing are current as of the date of execution below and that these individuals are authorized to sign contracts and other legally binding documents related to contracts with the Commonwealth of Massachusetts on behalf of the Contractor. I understand and agree that the Contractor has a duty to ensure that this listing is immediately updated and communicated to any state department with which the Contractor does business whenever the authorized signatories above retire, are otherwise terminated from the Contractor's employ, have their responsibilities changed resulting in their no longer being authorized to sign contracts with the Commonwealth or whenever new signatories are designated.

John Cordeiro
Signature

Date: 4/9/2020

Title: Vice President

Telephone: 339-987-5525

Fax: 339-987-5528

Email: jcordeiro@baincor.com

[Listing can not be accepted without all of this information completed.]

A copy of this listing must be attached to the "record copy" of a contract filed with the department.

Massachusetts Department of Transportation
CONTRACTOR AUTHORIZED SIGNATORY LISTING

Issued May 2004

CONTRACTOR LEGAL NAME: Bain Cor, Inc.
CONTRACTOR VENDOR/CUSTOMER CODE: VC0000506451

PROOF OF AUTHENTICATION OF SIGNATURE

It is a requirement of MassDOT to obtain authentication of signatures for all signatories listed on the attached Contractor Authorized Listing

This Section MUST be completed by the Contractor Authorized Signatory in presence of notary.

Signatory's full legal name (print or type): JOHN CORDEIRO

Title: Vice President

X John Cordeiro

Signature as it will appear on contract or other document (Complete only in presence of notary):

AUTHENTICATED BY NOTARY OR CORPORATE CLERK (PICK ONLY ONE) AS FOLLOWS:

I, Brian T McNeil (NOTARY) as a notary public certify that I witnessed the signature of the aforementioned signatory above and I verified the individual's identity on this date:

March 19, 20 20.

My commission expires on: 11-08-24

BRIAN T MCNEIL
Notary Public
Commonwealth of Massachusetts
My Commission Expires
AFFIX NOTARY SEAL

I, Wayne Bain (CORPORATE CLERK) certify that I witnessed the signature of the aforementioned signatory above, that I verified the individual's identity and confirm the individual's authority as an authorized signatory for the Contractor on this date:

3-19, 20 20.

AFFIX CORPORATE SEAL

Agency Head:

Signature

Colonel Christopher S. Mason #2401
(Type or Print Name and Title)

Chris.Mason@pol.state.ma.us
e-mail address

By signing above, I acknowledge that I have read and understand the job duties described in Appendix B

CJIS Representative:

Capt. Donald J. Cormier #812
Signature

Donald J. Cormier Captain
(Type or Print Name and Title)

donald.Cormier@pol.state.ma.us
e-mail address

By signing above, I acknowledge that I have read and understand the job duties described in Appendix C

Backup CJIS Representative:

Signature

Captain Bruce F. Hiorns
(Type or Print Name and Title)

Bruce.Hiorns@pol.state.ma.us
e-mail address

By signing above, I acknowledge that I have read and understand the job duties described in Appendix B

CJIS Technical/Security Contact:

Signature

(Type or Print Name and Title)

e-mail address

By signing above, I acknowledge that I have read and understand the job duties described in Appendix C

*Please only fax **pages eight (8) and nine (9) of this document** to 617.884.4601 or mail to CSS Unit of DCJIS*

CJIS User Agreement – Acknowledgement

Type or Print Agency Name: MSP- GHQ Date: 1-12-21

As a terminal agency utilizing the CJIS and NCIC systems, we hereby certify that we have read the User Agreement and acknowledge the duties and responsibilities as outlined in this document, as well as those documents incorporated by reference. We acknowledge that these duties and responsibilities have been developed and approved by the DCJIS in order to ensure the security, reliability, confidentiality, completeness and accuracy of all records contained in, or obtained by means of the CJIS and NCIC systems. We further acknowledge that failure to comply with these duties and responsibilities will subject this agency to various sanctions as approved by the DCJIS. These sanctions may include the termination of CJIS services.

List the ORI and the Agency code for all terminals [Available via QLIST] covered by this User Agreement

	ORI # (ex: MA0010100)	**Agency Code** (ex: CAM)
1.	MAMSP0000	GHQ
2.		
3.		
4.		
5.		

List the type and quantity of mobile devices used by your agency covered by this User Agreement and any agencies in which a MOU may be applicable. (Include additional pages if necessary):

Agency Name	**Type**	**Quantity**

COMMONWEALTH TERMS AND CONDITIONS

This Commonwealth Terms and Conditions form is jointly issued by the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) for use by all Commonwealth of Massachusetts ("State") Departments and Contractors. ***Any changes or electronic alterations by either the Department or the Contractor to the official version of this form, as jointly published by ANF, CTR and OSD, shall be void.*** Upon execution of the Standard Contract Form these Commonwealth Terms and Conditions will be incorporated by reference. Performance shall include services rendered, obligations due, costs incurred, commodities and deliverables provided and accepted by the Department, programs provided or other commitments authorized under a Contract. A deliverable shall include any tangible product to be delivered as an element of performance under a Contract. The Commonwealth is entitled to ownership and possession of all deliverables purchased or developed with State funds. Contract shall mean the Standard Contract Form issued jointly by ANF, CTR and OSD.

1. *Contract Effective Start Date.* Notwithstanding verbal or other representations by the parties, the effective start date of performance under a Contract shall be the later of the date the Contract was executed by an authorized signatory of the Contractor, the date the Contract was executed by an authorized signatory of the Department, the date specified in the Contract, or the date of any approvals required by law or regulation.

2. *Payments And Compensation.* The Contractor shall only be compensated for performance delivered and accepted by the Department in accordance with the specific terms and conditions of a Contract. All Contract payments are subject to appropriation pursuant to M.G.L. c. 29, § 26, or the availability of sufficient non-appropriated funds for the purposes of a Contract, and shall be subject to intercept pursuant to M.G.L. c. 7A, § 3 and 815 CMR 9.00. Overpayments shall be reimbursed by the Contractor or may be offset by the Department from future payments in accordance with state finance law. Acceptance by the Contractor of any payment or partial payment, without any written objection by the Contractor, shall in each instance operate as a release and discharge of the State from all claims, liabilities or other obligations relating to the performance of a Contract.

3. *Contractor Payment Mechanism.* All Contractors will be paid using the Comptroller's payment system unless a different payment mechanism is required. The Contractor shall timely submit invoices and supporting documentation as prescribed in a Contract. The Department shall review and return rejected invoices within fifteen (15) days of receipt with a written explanation for rejection. Payments shall be made in accordance with the bill paying policy issued by the Office of the Comptroller and 815 CMR 4.00, provided that payment periods listed in a Contract of less than forty-five (45) days from the date of receipt of an invoice shall be effective only to enable a Department to take advantage of early payment incentives and shall not subject any payment made within the forty-five (45) day period to a penalty. The Contractor Payroll System shall be used only for Individual Contractors who have been determined to be Contract Employees as a result of the Department's completion of an Internal Revenue Service SS-8 form in accordance with the Omnibus Budget Reconciliation Act (OBRA) 1990, and shall automatically process all state and federal mandated payroll, tax and retirement deductions.

4. *Contract Termination Or Suspension.* A Contract shall terminate on the date specified in a Contract, unless this date is properly amended in accordance with all applicable laws and regulations prior to this date, or unless terminated or suspended under this Section upon prior written notice to the Contractor. The Department may terminate a Contract without cause and without penalty, or may terminate or suspend a Contract if the Contractor breaches any material term or condition or fails to perform or fulfill any material obligation required by a Contract, or in the event of an elimination of an appropriation or availability of sufficient funds for the purposes of a Contract, or in the event of an unforeseen public emergency mandating immediate Department action. Upon immediate notification to the other party, neither the Department nor the Contractor shall be deemed to be in breach for failure or delay in performance due to Acts of God or other causes factually beyond their control and without their fault or negligence. Subcontractor failure to perform or price increases due to market fluctuations or product availability will not be deemed factually beyond the Contractor's control.

5. *Written Notice.* Any notice shall be deemed delivered and received when submitted in writing in person or when delivered by any other appropriate method evidencing actual receipt by the Department or the Contractor. Any written notice of termination or suspension delivered to the Contractor shall state the effective date and period of the notice, the reasons for the termination or suspension, if applicable, any alleged breach or failure to perform, a reasonable period to cure any alleged breach or failure to perform, if applicable, and any instructions or restrictions concerning allowable activities, costs or expenditures by the Contractor during the notice period.

6. *Confidentiality.* The Contractor shall comply with M.G.L. c. 66A if the Contractor becomes a "holder" of "personal data". The Contractor shall also protect the physical security and restrict any access to personal or other Department data in the Contractor's possession, or used by the Contractor in the performance of a Contract, which shall include, but is not limited to, the Department's public records, documents, files, software, equipment or systems.

7. *Record-keeping And Retention, Inspection Of Records.* The Contractor shall maintain records, books, files and other data as specified in a Contract and in such detail as shall properly substantiate claims for payment under a Contract, for a minimum retention period of six (6) years beginning on the first day after the final payment under a Contract, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving a Contract. The Department shall have access, as well as any parties identified under Executive Order 195, during the Contractor's regular business hours and upon reasonable prior notice, to such records, including on-site reviews and reproduction of such records at a reasonable expense.

8. *Assignment.* The Contractor may not assign or delegate, in whole or in part, or otherwise transfer any liability, responsibility, obligation, duty or interest under a Contract, with the exception that the Contractor shall be authorized to assign present and prospective claims for money due to the Contractor pursuant to a Contract in accordance with M.G.L. c. 106, § 9-318. The Contractor must provide sufficient notice of assignment and supporting documentation to enable the Department to verify and implement the assignment. Payments to third party assignees will be processed as if such payments were being made directly to the Contractor and these payments will be subject to intercept, offset, counter claims or any other Department rights which are available to the Department or the State against the Contractor.

9. *Subcontracting By Contractor.* Any subcontract entered into by the Contractor for the purposes of fulfilling the obligations under a Contract must be in writing, authorized in advance by the Department and shall be consistent with and subject to the provisions of these Commonwealth Terms and Conditions and a Contract. Subcontracts will not relieve or discharge the Contractor from any duty, obligation, responsibility or liability arising under a Contract. The Department is entitled to copies of all subcontracts and shall not be bound by any provisions contained in a subcontract to which it is not a party.

10. *Affirmative Action, Non-Discrimination In Hiring And Employment.* The Contractor shall comply with all federal and state laws, rules and regulations promoting fair employment practices or prohibiting employment discrimination and unfair labor practices and shall not discriminate in the hiring of any applicant for employment nor shall any qualified employee be demoted, discharged or otherwise subject to discrimination in the tenure, position, promotional opportunities, wages, benefits or terms and conditions of their employment because of race, color, national origin, ancestry, age, sex, religion, disability,

COMMONWEALTH TERMS AND CONDITIONS

handicap, sexual orientation or for exercising any rights afforded by law. The Contractor commits to purchasing supplies and services from certified minority or women-owned businesses, small businesses or businesses owned by socially or economically disadvantaged persons or persons with disabilities.

11. *Indemnification.* Unless otherwise exempted by law, the Contractor shall indemnify and hold harmless the State, including the Department, its agents, officers and employees against any and all claims, liabilities and costs for any personal injury or property damages, patent or copyright infringement or other damages that the State may sustain which arise out of or in connection with the Contractor's performance of a Contract, including but not limited to the negligence, reckless or intentional conduct of the Contractor, its agents, officers, employees or subcontractors. The Contractor shall at no time be considered an agent or representative of the Department or the State. After prompt notification of a claim by the State, the Contractor shall have an opportunity to participate in the defense of such claim and any negotiated settlement agreement or judgment. The State shall not be liable for any costs incurred by the Contractor arising under this paragraph. Any indemnification of the Contractor shall be subject to appropriation and applicable law.

12. *Waivers.* Forbearance or indulgence in any form or manner by a party shall not be construed as a waiver, nor in any way limit the legal or equitable remedies available to that party. No waiver by either party of any default or breach shall constitute a waiver of any subsequent default or breach.

13. *Risk Of Loss.* The Contractor shall bear the risk of loss for any Contractor materials used for a Contract and for all deliverables, Department personal or other data which is in the possession of the Contractor or used by the Contractor in the performance of a Contract, until possession, ownership and full legal title to the deliverables are transferred to and accepted by the Department.

14. *Forum, Choice of Law And Mediation.* Any actions arising out of a Contract shall be governed by the laws of Massachusetts, and shall be brought and maintained in a state or federal court in Massachusetts which shall have exclusive jurisdiction thereof. The Department, with the approval of the Attorney General's Office, and the Contractor may agree to voluntary mediation through the Massachusetts Office of Dispute Resolution (MODR) of any Contract dispute and will share the costs of such mediation. No legal or equitable rights of the parties shall be limited by this Section.

15. *Contract Boilerplate Interpretation, Severability, Conflicts With Law, Integration.* Any amendment or attachment to any Contract which contains conflicting language or has the effect of a deleting, replacing or modifying any printed language of these Commonwealth Terms and Conditions, as officially published by ANF, CTR and OSD, shall be interpreted as superseded by the official printed language. If any provision of a Contract is found to be superseded by state or federal law or regulation, in whole or in part, then both parties shall be relieved of all obligations under that provision only to the extent necessary to comply with the superseding law; provided however, that the remaining provisions of the Contract, or portions thereof, shall be enforced to the fullest extent permitted by law. All amendments must be executed by the parties in accordance with Section 1 of these Commonwealth Terms and Conditions and filed with the original record copy of a Contract as prescribed by CTR. The printed language of the Standard Contract Form, as officially published by ANF, CTR and OSD, which incorporates by reference these Commonwealth Terms and Conditions, shall supersede any conflicting verbal or written agreements relating to the performance of a Contract, or attached thereto, including contract forms, purchase orders or invoices of the Contractor. The order of priority of documents to interpret a Contract shall be as follows: the printed language of the Commonwealth Terms and Conditions, the Standard Contract Form, the Department's Request for Response (RFR) solicitation document and the Contractor's Response to the RFR solicitation, excluding any language stricken by a Department as unacceptable and including any negotiated terms and conditions allowable pursuant to law or regulation.

IN WITNESS WHEREOF, the Contractor certifies under the pains and penalties of perjury that it shall comply with these Commonwealth Terms and Conditions for any applicable Contract executed with the Commonwealth as certified by their authorized signatory signing the Standard Contract Form.

TRAFFIC SAFETY

RESOURCE GUIDE



IACP
International Association of Chiefs of Police

Cover Images Credits: National Sheriffs' Association and the New York State Police

Version: October 2020

Disclaimer:

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The United States Government assumes no liability for its content or use thereof. If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

INTRODUCTION

Police officers in the United States today know all too well how challenging it has become to ensure the safe movement of traffic on the roadways. Factors such as distracted driving, both alcohol *and* drug-impaired motorists, an increase in total miles driven, and newly emerging considerations such as autonomous vehicles, promoting traffic safety as a national priority has become even more complex.

The **Traffic Safety Resource Guide** is designed to help law enforcement officers to address the elements of traffic safety from education to enforcement as well as share research and best practices. The Guide provides promising practices to support leaders in responding to traffic safety issues they are encountering in their communities. While the Guide does not seek to address all of the issues, it serves as a source of potential strategies that can be implemented, while also providing the latest research. The Guide can also serve as a starting point for learning more about ongoing research and studies by trusted organizations with a long history of commitment to traffic safety.

The Guide is written for police officers. In fact, many of the contributors to the Guide are currently working in the field of traffic safety – police officers, researchers, practitioners and others who best understand what the key issues are. The IACP has learned anecdotally that police officers have been known to carry the Guide in their patrol vehicle trunk, while at the same time, police chiefs use the Guide in planning for meetings with their city manager, elected officials, and community groups.

As you review the Guide, please keep in mind that new traffic safety initiatives and research are emerging almost daily. The IACP, working with NHTSA, plans to develop a future electronic version of the Traffic Safety Resource Guide, possibly in either a webpage or app format. This will help facilitate near real-time updates of data and research while also providing a mobile platform for smartphones and tablets. Feel free to contact the IACP and NHTSA with more specific questions related to traffic safety that may not be addressed in this Guide.

The mission you have undertaken of ensuring safe motor vehicle travel on the many roads in your communities can be a very challenging task. By working together and harnessing the resources and best practices mentioned in the **Traffic Safety Resource Guide**, the IACP's goal is to enable law enforcement leaders to meet and exceed their traffic safety initiatives.

TABLE OF CONTENTS

5 Chapter 1: Reduction of Traffic Crashes
5 Alcohol and Drug-Impaired Driving
10 Current Issues in Drug Impaired Driving
13 Distracted Driving
14 Drowsy Driving
15 Aggressive Driving
16 Young Drivers
17 Older Drivers
19 Bicycle and Pedestrian Safety
21 Motorcycle Safety
22 Special Enforcement Initiatives to Reduce Crashes
24 Traffic Safety through High Visibility Enforcement
26 The Importance of Occupant Protection

30 Chapter 2: Officer Safety
30 Research in Brief: Officer-Involved Collisions: Magnitude, Risk Factors, and Prevention
31 Safety for Law Enforcement Officers – Still a Priority
33 Below 100 Initiative: A Reality Check on Officer Safety
34 Destination Zero Program
35 Police Pursuits: Trends and Emerging Technology
36 The Dangers of Vehicle Pursuits: New Emerging Issues
40 Move Over Law
40 Officer Safety, Predictive Policing, and Community Relations
42 Tactical Common Sense: Saving Lives with Seatbelts and Traffic Safety Vests

45 Chapter 3: Allocation, Deployment, and Evaluation of Traffic Personnel
45 Police Allocation Manual (PAM)
45 Using Traffic Safety Data to Drive Resource Allocation
47 The Changing of Culture as a Byproduct of the Delaware State Police's Implementation of the Stratified Model to Address Traffic Safety: The Pilot Study

52 Chapter 4: Crash Investigation

57 Chapter 5: Commercial Vehicles and Hazardous Materials Regulation
57 U.S. Department of Transportation

60 Chapter 6: The Driver Licensing System
60 The Driver Licensing System

64 Chapter 7: Registration, Title, and Inspection Enforcement
64 Registration, Title, and Inspection Enforcement

67 Chapter 8: Uniformity, Reciprocity, and Federal Programs
67 Federal Agencies and Grants
71 NHTSA Regional Offices
71 FHWA Field Services and Resource Centers

72 Chapter 9: Emerging and Critical Issues in Traffic Safety
72 Traffic Safety's Critical Role in the Law Enforcement Mission
73 Traffic Enforcement: Back to Basics
78 Leading Traffic Safety
81 In Pursuit of Bias-Free Traffic Enforcement
86 Highly Automated and Connected Vehicles
88 Legalization of Marijuana: Issues for Traffic Safety
93 Are Red Light Cameras an Effective Crash-Reduction Solution?
97 Speed Cameras to Reduce Speeding Traffic and Road Traffic Injuries
98 Unmanned Aerial Systems and Traffic Safety
98 5 Ways NG911 Can Improve Your Agency
100 Public Relations and Messaging in the Digital Age
105 Traffic Incident Management (TIM)
107 The Incident Command System (ICS) and the National Incident Management System (NIMS)
108 Enforcement, Engineering, Education, and Evaluation

110 Chapter 10: Legal Issues in Traffic Safety
110 Legal Issues in Traffic Safety

116 Appendices
116 Appendix A: Bibliography of Resources
128 Appendix B: Associations and Committees
132 Appendix C: Abbreviations and Acronyms
137 Appendix D: Traffic Safety Resource Prosecutors

144 Acknowledgements

CHAPTER 1: REDUCTION OF TRAFFIC CRASHES

Alcohol- and Drug-Impaired Driving

In every state in the United States, it is illegal to drive with a BAC of .08 or higher, yet an average of one person is killed in a drunk-driving crash every 48 minutes. Every day, thirty people in the U.S. die in an alcohol-related vehicle crash. [1]

While the National Highway Traffic Safety Administration (NHTSA) advises that impaired driving fatalities have fallen by a third in the last three decades, the risk of being involved in an alcohol-impaired crash is still one-in-three over the course of an individual's lifetime. Impaired driving fatalities in the U.S. increased by 5.7 percent from 2015 to 2017. Parallel to the overall number of lives lost in traffic crashes in 2015, the number of alcohol-impaired fatalities also rose 5.8 percent from 2015 to 2017. [2] (See Table: Fatalities and Fatality Rate per 100 Million Vehicle Miles Traveled in Alcohol-Impaired Driving Crashes, 2008-2017)

Meanwhile, the use of marijuana and prescription drugs has become even more prominent among drivers on U.S. roads, raising more challenges for traffic safety officials. With the legalization of cannabis in several states for medical or recreational purposes, the increased prevalence of drugged driving is likely to result in more deaths on roadways. More studies and research are needed, so law enforcement can prepare effective and efficient strategies related to drug-impaired motorists.

A NHTSA report indicated that the prevalence of marijuana in drivers in Washington State has increased significantly since the implementation of legal marijuana retail sales in 2014. During the daytime, when children and the elderly are more likely to be outside, the rate of THC identification in drivers more than doubled from 7.8 percent prior to cannabis legalization to 18.9 percent one year after legalization. [3]

A second survey considered whether marijuana use by drivers was associated with a greater risk of crash involvement. Results from the survey found that marijuana users were more likely to be involved in crashes, but that the increased risk was due in part to the potential for marijuana users to be in groups already at a higher risk of crashes, such as young men. [4] More data is needed on the link between marijuana use and the propensity of a higher incidence of crashes.

Most law enforcement officers in the U.S. do not test impaired drivers for drugs unless the motorists' blood or breath sample results are below the legal limit for alcohol. This is a standard operating procedure to save time and expenses associated with the testing process. Many times, drivers who have been involved in crashes have the presence of both alcohol and drugs in their system. [5] Without more established practices of testing for drug impaired driving, the true picture of drug-impaired driving will remain unknown.

Another complex and emerging issue related to drug-impaired driving is the significant increase in the use of prescription drugs. The abuse of opiate drugs specifically has received national attention as the United States is in the midst of an opioid overdose epidemic. The Centers for Disease Control and Prevention (CDC) reported in 2017 that 70,200 deaths were caused by prescription opioids and heroin – an all-time record. [6] As the instances involving the abuse of these drugs increases, law enforcement must be prepared to combat an

Fatalities and Fatality Rate per 100 Million VMT in Alcohol-Impaired-Driving Crashes, 2008–2017



Sources: Fatalities – FARS 2008–2016 Final File, 2017 ARF; 2008–2016 VMT – Federal Highway Administration's (FHWA) Annual Highway Statistics; 2017 VMT – FHWA's Traffic Volume Trends (May 2018)

increasing number of opioid-impaired people in the driving population.

Clearly, the data on alcohol and drug-impaired driving is very concerning. There has been a documented increased in the prevalence of drugged driving in the U.S. In fact, the number of drivers involved in fatal motor vehicle crashes who have tested positive for drugs increased from 28 percent in 2005 to 32 percent in 2012. [7] NHTSA has been a leader in working diligently to develop evidence-based and data-driven initiatives. Through research, public awareness campaigns, and the many state safety grant programs, NHTSA's goal is to eliminate alcohol- and drug-impaired driving. NHTSA has been working with various partners, including the IACP, GHSA, NSA, MADD, and law enforcement across the U.S. NHTSA regularly partners with law enforcement on successful campaigns to address impaired driving, such as Drive Sober or Get Pulled Over, Buzzed Driving is Drunk Driving, and The Ultimate Party Foul initiatives. More information regarding these campaigns on the NHTSA website at https://www.nhtsa.gov/ or on the IACP website at http://www.theiacpthelACP.org/trafficsafety.

The IACP Provides Leadership in Addressing Alcohol and Drug-Impaired Driving

Strong leadership in law enforcement is the first key to success in bolstering efforts to eliminate impaired driving. Ensuring that traffic enforcement resources are appropriately focused and agencies' field activities support desired outcomes is crucial to the success of the traffic safety mission. Chief executives who emphasize the link between education and enforcement with their rank and file officers will serve as a catalyst to motivate key partners beyond law enforcement.

The Broken Windows Model of policing demonstrated the opportunity to reduce crime and improve quality of life by addressing seemingly insignificant crimes, which thereby allowed law enforcement to deter people from committing larger crimes and drive down the general crime rate. There are concepts exhibited through the implementation of this theory into policing that are easily transferrable to traffic enforcement. [8] One research project conducted by Weiss recommended law enforcement agencies "to consider enhancing or expanding their use of traffic enforcement teams because of their potential value in reducing public order crimes." [9] Jurisdictions that have implemented a "Fixing Broken Windows" strategy can reinforce these concepts to contribute to the reduction of impaired driving.

In addition to ensuring aggressive impaired driving enforcement is occurring in their agencies, law enforcement agencies should consider:

- Developing strong support among government leaders;
- Sponsoring or participating in meaningful awards and recognition programs to provide positive reinforcement for impaired driving enforcement; and
- Publicly supporting advancements in automotive and enforcement technology for sensing impairment.

Criminal Justice Collaboration

Partnering and collaborating with other agencies and organizations in order to combine resources can serve as a "force multiplier," and achieve results that a single agency could not accomplish alone. There are excellent examples of innovative campaigns that approach the challenge of impaired driving from a multi-disciplined standpoint, incorporating education, awareness, and enforcement.

One such campaign is the High Visibility Education and Enforcement (HVEE) Pilot Project. While not focused only upon impaired driving, this project assembled partners from NHTSA, the IACP, the Governors Highway Safety Association (GHSA), the U.S. Department of Transportation to help reduce traffic deaths through HVEE initiatives. Four states – Delaware, Maryland, North Carolina, and Wisconsin – participated in this IACP-led effort with programs addressing specific localized traffic safety concerns. The HVEE concept offers an evidence-based, data-driven, problem-solving approach that combined proactive public education campaigns to raise awareness of the identified safety issue, followed by targeted enforcement involving multiple law enforcement agencies. One of the hallmarks of the program was the opportunity to collaborate with stakeholders from multiple disciplines, including representatives from state transportation organizations, state highway safety associations, and state, county, and municipal law enforcement agencies. A summary of each state's HVEE program and checklists for high visibility enforcement are available here: www.theiacp.org/HVEE. Additional examples of projects like the HVEE program are also located in the Bibliography of Resources section in the Appendix.

Public and private partnerships can help break traditional boundaries, provide broad-based support, amplify available resources and establish shared ownership. NHTSA, the IACP, and other key partners will continue to provide resources and research to law enforcement leaders to assist them in their development and implementation of impaired driving reduction strategies. These efforts, and the engagement of law enforcement agencies throughout the country, will be needed to overcome the multi-faceted challenge of impaired driving.

Effective Communication Strategies

Effective internal and external communication is another key to success in emphasizing law enforcement's efforts to eliminate impaired driving. Law enforcement leaders must take affirmative measures to "sell" impaired driving enforcement to both their officers and the public. Garnering the support and response of officers and the public requires leadership, which begins with awareness and commitment at the highest level of any organization. Motivating line-level officers to not only accept, but also become actively involved with impaired driving enforcement should be one of the focal points of any agency's traffic enforcement program. This motivation begins with the chief, sheriff, or other agency head and must be conveyed from the top-down throughout all levels of the organization.

Similarly, external communications are essential to success. Law enforcement executives should not be deterred by the occasional negative public response to impaired driving enforcement. In one example, the *Chicago Tribune* wrote an article entitled "Sobriety checkpoints yield thousands of minor citations but few DUI arrests." [10] A consensus of the vast body of research on public attitudes continues to show that the public rates impaired driving among the greatest traffic safety threats; additionally, there is broad-based support for enhanced enforcement. Impaired driving enforcement programs are greatly enhanced when an agency is proactive in garnering support for its efforts from key supporters and allies, such as MADD, as well as other traffic safety organizations, community groups, and coalitions. [11]

Two key partners are the State Highway Safety Office (SHSO) in each state, as well as, the Governors Highway Safety Association (GHSA). GHSA is an umbrella organization representing the interests of the SHSOs and serves as the state's voice on highway safety at the national level. Working collaboratively, the SHSOs and the GHSA facilitate innovative education and awareness campaigns and are highly recommended partners for any chief executive. NHTSA, SHSOs, and GHSA all provide template media materials on their websites that can be extremely valuable to law enforcement. [12] Refer here https://www.trafficsafetymarketing.gov/ for more information.

Impaired Driving Detection

Law enforcement officers utilize various practices and advanced technologies to detect impaired drivers. This section will summarize some of the more common methods and technologies used in the field.

Standardized Field Sobriety Testing

Developed in the late 1970's and early 1980's, the Standardized Field Sobriety Test (SFST) battery consists of tests administered and evaluated in a standardized manner to obtain validated indicators of impairment and establish probable cause for arrest.

A formal program of training was developed and is available through NHTSA to help law enforcement officers become more skillful at detecting DUI suspects, describing the behavior of these suspects, and presenting effective testimony in court. Formal administration and accreditation of the program is provided through the IACP. SFST training prepares law enforcement officers to use the standard test battery to enhance the prosecution of impaired driving cases.

The three tests comprising the SFST are (1) the horizontal gaze nystagmus (HGN), (2) the walk-and-turn, and (3) the one-leg stand. These tests are administered systematically and are evaluated according to measured responses of the driver. [13]

Consult the IACP and NHTSA for additional information regarding the SFST training curriculum and your local or state training centers for available classes.

Drug Recognition Expert (DRE) Program

A drug recognition expert (DRE) is a law enforcement officer trained to recognize impairment in drivers under the influence of drugs other than, or in addition to, alcohol. The IACP coordinates the International Drug Evaluation and Classification (DEC) Program with support from NHTSA. In addition to certifying law enforcement officers as DREs, the DEC Program educates prosecutors and judges in the prosecution of drugged drivers. [14] For more information on the DEC Program and DREs, visit www.decp.org. Also see *"Current Issues in Drug Impaired Driving"* by Lieutenant Matt Myers, Peachtree City Police Department, at the end of this chapter.

Advanced Roadside Impaired Driving Enforcement (ARIDE)

The Advanced Roadside Impaired Driving Enforcement (ARIDE) program was developed by NHTSA with input from the IACP Technical Advisory Panel (TAP) and the Virginia Association of Chiefs of Police (VACP). ARIDE was created to address the gap in training between the SFST and DRE training. The ARIDE program also stresses the importance of securing the most appropriate biological sample in order to identify substances likely causing impairment. [15] Additional information is available at this website: http://www.decp.org/training/. Another key resource is the article entitled *"Current Issues in*

Drug Impaired Driving" by Lieutenant Matt Myers of the Peachtree City, Georgia, Police Department, at the end of this chapter.

Roadside and Sobriety Checkpoints

Roadside checkpoints provide law enforcement personnel with a ready means to monitor and check driver condition, driver's licenses, insurance, vehicle registrations, and compliance with other laws regarding vehicle operation. Although federal case law supports the use of checkpoints in this manner (subject to certain restrictions), law enforcement executives should educate themselves on the state laws regarding the use of checkpoints before implementing such operations in their jurisdiction.

Because some courts and licensing authorities now issue restricted licenses to offenders, roadside checks allow officers to monitor compliance with court-ordered and statutory restrictions. Law enforcement personnel can contact increased numbers of vehicle operators without first having to make traffic stops. Roadside checkpoints also enable officers to conduct vehicle registration inquiries and detect uninspected or unsafe vehicles.

A sobriety checkpoint is a highly visible enforcement mechanism. All motorists approaching a designated area of a highway are stopped and briefly investigated for signs of intoxication. Due to legal issues, not all state laws allow law enforcement to conduct sobriety checkpoints. Some states have laws authorizing their use while others forbid them entirely; thus, law enforcement leadership should be cognizant of their state and jurisdictional laws and regulations.

The HSC and NHTSA have published operational guidelines that chief executives should be familiar with to ensure their personnel follow them closely, as well as make certain all officers conduct the checkpoints in a safe, legal, and effective manner. These guidelines suggest that checkpoints should be part of an ongoing program to combat impaired driving, have local judicial support, and conform to agency policy. The location should be pre-selected by management based upon statistics and should have special advance warning devices, a visible police presence, chemical testing logistics, contingency planning, effective detection and investigation techniques, operational briefings, comprehensive public information and public education efforts, and post-incident critiques based on data collection and evaluation. [16] Law enforcement leaders should contact the traffic safety resource prosecutor (TSRP) or SHSO in their state for assistance in developing policies and practices consistent with state and federal laws regarding road checks. Refer to the Appendix for a listing of TSRPs in each state.

Breath-Testing Instruments

The NHTSA Alcohol Countermeasures Program (ACP) provides continued support to further reduce the rate of intoxicated driving through the development and evaluation of measurement techniques for alcohol on the breath, production of performance guidelines for breath measurement devices, testing of instruments intended for police use, and technical support of demonstration and research programs.

Under Section 403 of the Highway Safety Act of 1966, the Secretary of Transportation is required to carry out a research and demonstration program. In the area of alcohol breath testing, the requirements of the Act are met by NHTSA through the Office of Research and Program Development and the Office of Behavioral Safety Research. Supported by a capable laboratory, they are responsible for the development and evaluation of test procedures and related instrumentation. [17]

The Alcohol Countermeasures Laboratory (ACL) evaluates alcohol devices according to NHTSA's Model Specifications for evidential breath testers, alcohol screening devices, and calibrating units. Devices that meet the specifications are added to NHTSA's Conforming Products List (CPL), which is available on the NHTSA website.

The ACL also evaluates other alcohol test devices of interest for potential usefulness in alcohol-impaired countermeasures, including ignition interlock devices, disposable or re-useable personal breath testers, passive breath testers, or devices that test other fluids for alcohol (e.g., saliva testers). [18] A comprehensive list may be found at the Alcohol Measuring Device Testing and Technical Information page: https://www.volpe.dot.gov/safety-management-and-human-factors/surface-transportation-human-factors/alcohol-measuring-device. [19]

Law enforcement leaders should be cognizant of state guidelines for testing instruments. Some states only allow preliminary testing to be conducted with a device approved by a specific agency, such as the state's forensic science laboratory.

Preliminary (or Portable) Breath Test Devices (PBT)

The preliminary (or portable) breath test (PBT) device is an instrument used for the purpose of breath alcohol screening in the field. A law enforcement officer can use the PBT as a preliminary screening tool for impaired driving by having the suspected driver provide a breath sample for an instantaneous determination of breath alcohol content.

Officers are reminded to refer to their applicable state and local laws regarding the use of evidence from a PBT. While results are generally not admissible as evidence of impairment, they do provide officers with additional objective information to establish probable cause for arrest and further chemical testing. [20]

Non-Invasive or Passive Alcohol Sensors

Passive alcohol sensors (PAS) are instruments that detect the presence of alcohol in normally expelled breath, and they require no cooperation from the driver. During a roadside interview of the driver, the officer places the sensor within six inches of the driver's mouth. It contains a small fan which samples the ambient air for examination. An electro-chemical mechanism analyzes the air for the presence of alcohol. [21]



From: https://goo.gl/images/QxLBNL

Some sensors are concealed within a flashlight or a clipboard, which can be used as a passive or active detector. NHTSA studies indicate these devices are effective during sobriety checkpoints when the decision to further evaluate drivers must be made expeditiously.

Vehicle-Based Sensors of Driver Behavior to Detect Impairment

Although enforcement and educational approaches have helped to reduce alcohol-impaired driving fatalities, new vehicle-based sensor technologies are being studied by NHTSA and other interested groups. One such approach concerns countermeasures that capitalize on the increasingly sophisticated sensor and computational platform that is available on many production vehicles. Such vehicle-based countermeasures have the potential to address alcohol-impaired driving and save thousands of lives each year. Vehicle-based countermeasures use sensors that describe drivers' control inputs (e.g., steering wheel and brake pedal movement), vehicle state (e.g., accelerometer and lane position), driving context (e.g., speed zone information and proximity of surrounding vehicles), and driver state (e.g., eye movements and posture). Data from these sensors can be transformed, combined, and processed with a variety of algorithms to develop a detailed description of the driver's response to the roadway. These sensors and algorithms hold promise for identifying a range of driver impairments, including distraction, drowsiness, and even age-related cognitive decline. Alcohol represents a particularly important impairment that might be detected by vehicle-based sensors and algorithms. [22]

For more information on one vehicle-based sensor study conducted by NHTSA, refer to this website: https://www-esv.nhtsa.dot.gov/Proceedings/22/files/22ESV-000322.pdf.

Alcohol Ignition Interlock

One effective strategy in addressing the problem of impaired driving, which has application to both first-time and repeat offenders, is the use of ignition interlock devices. An ignition interlock device is an after-market technology device installed in a motor vehicle to prevent a driver from operating the vehicle if the driver has been drinking.

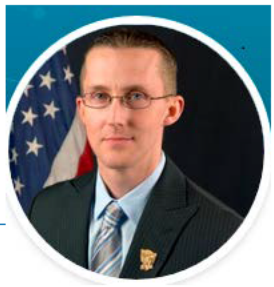
A driver must submit a breath sample using the device before it will operate. If the driver's blood-alcohol content (BAC) is over a pre-set limit, the ignition interlock will not allow the vehicle to start. Studies have shown that these devices are effective in reducing subsequent arrests for driving under the influence among both first-time and repeat offenders, with reported reductions ranging from 50-90 percent while the interlock device is installed on the vehicle. From a law enforcement perspective, it is important for officers to be able to determine offenders who were sentenced to an ignition interlock program while in the field. One suggestion is to have a special designation or endorsement on an offender's license that is easily identifiable by a law enforcement officer. [24]

Notes:

1. National Highway Traffic Safety Administration, "Drunk Driving," https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812630.
2. National Center for Statistics and Analysis, "Alcohol-Impaired Driving: 2017 Data," *Traffic Safety Facts* (NHTSA, November 2018), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812630.
3. A. Ramirez et al., "Technology Transfer Series: Drivers' Use of Marijuana in Washington State," *Traffic Tech* (NHTSA, August 2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812307-tt-marijuana_use_in_wa.pdf. (accessed February 3, 2017).
4. National Highway Traffic Safety Administration, "Drugged Driving," https://www.nhtsa.gov/risky-driving/drugged-driving (accessed February 3, 2017).
5. John Flannigan, Stephen K. Talpins, and Christina Moore, "Oral Fluid Testing for Impaired Driving Enforcement," *The Police Chief* 84, no. 1 (January 2017): 58-63, http://www.policechiefmagazine.org/oral-fluid-testing-for-impaired-driving-enforcement/?ref=f51308af5da285f21d878208a11e3ff5 (accessed February 3, 2017).
6. U.S. Centers for Disease Control and Prevention, "Injury Prevention & Control: Opioid Overdose," https://www.cdc.gov/drugoverdose/.
7. National Center for Statistics and Analysis, "Drug Involvement of Fatally Injured Drivers," *Traffic Safety Facts* (NHTSA, November 2010), (accessed February 3, 2017).

8. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811415. (accessed February 3, 2017).
9. Impaired Driving Subcommittee, "Impaired Driving Guidebook: Three Keys to Renewed Focus and Success," International Association of Chiefs of Police, 2006, http://www.theiacp.org/portals/0/pdfs/ImpairedDrivingGuidebook.pdf. (accessed February 3, 2017).
10. Marc Weiss, "Traffic Enforcement, Policing and Crime Rates," Walden University ScholarWorks, 2016, http://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=3731&context=dissertations. (accessed February 3, 2017).
11. Angela Caputo, "Sobriety Checkpoints Yield Thousands of Minor Citations but Few DUI Arrests," *Chicago Tribune,* May 8, 2015, http://www.chicagotribune.com/news/watchdog/ct-dui-checkpoints-suburbs-met-20150507-story.html (accessed February 14, 2017).
12. Impaired Driving Subcommittee, "Impaired Driving Guidebook: Three Keys to Renewed Focus and Success," International Association of Chiefs of Police, 2006, http://www.theiacp.org/portals/0/pdfs/ImpairedDrivingGuidebook.pdf.
13. Ibid.
14. *Highway Safety Desk Book* (n.p., 2004), 5–7 – 5–9, https://ntl.bts.gov/DOCS/deskbk.html.
15. International Association of Chiefs of Police, "IACP DEC Program: International Drug Evaluation and Classification Program," http://www.decp.org/ (accessed February 3, 2017).
16. ———, "Training." http://www.decp.org/training/ (accessed February 3, 2017).
17. *Highway Safety Desk Book* (n.p., 2004), 5–11 – 5–14, https://ntl.bts.gov/DOCS/deskbk.html.
18. Volpe, "Alcohol Countermeasures Help Reduce Intoxicated Driving," National Transportation Systems Center, October 31, 2013, https://www.volpe.dot.gov/safety-management-and-human-factors/surface-transportation-human-factors/alcohol-countermeasures (accessed February 3, 2017).
19. Ibid.
20. Ibid.
21. *Highway Safety Desk Book* (n.p., 2004), 5–24, https://ntl.bts.gov/DOCS/deskbk.html.
22. *Highway Safety Desk Book* (n.p., 2004), 5–25, https://ntl.bts.gov/DOCS/deskbk.html.
23. John D. Lee et al., "Assessing the Feasibility of Vehicle-Based Sensors to Detect Alcohol Impairment," (NHTSA, August 2010), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/811886-assess_veh-based_sensors_4_drowsy-driving_detection.pdf. (accessed February 3, 2017).
24. Karen Sprattler, "Ignition Interlocks - What You Need to Know," (NHTSA, November 2009), https://www.bing.com/cr?IG=E9C62525CC25419E896A2F08F9677C6A&CID=03271507FF6461EE0D4E1F26FE556023&rd=1&h=qPeO3BuTZk17q-R3zUaJPNirgRPm_KImtE1_FxfUVsU&v=1&r=https%3a%2f%2fwww.nhtsa.gov%2fstaticfiles%2fnti%2fimpaired_driving%2fpdf%2f811246.pdf&p=DevEx,5060.1 (accessed February 6, 2017).

Current Issues in Drug Impaired Driving



By: **Lieutenant Matt Myers,**
Peachtree City Police Department,
Peachtree City, Georgia

The 2013-2014 National Roadside Study of Alcohol and Drug Use by Drivers revealed an encouraging trend of declining alcohol use by drivers. [1] The data collected by this study, along with declining alcohol-related fatalities documented by the National Highway Traffic Safety Administration (NHTSA) Fatality Analysis Reporting System, demonstrate promising evidence that "drunk" driving education and enforcement initiatives are creating positive change. While it may be encouraging that the Roadside Survey found only 8.3 percent of drivers were positive for alcohol, law enforcement should take note that researchers found over 20 percent of drivers tested positive for at least one drug – an increase from the 16.3 percent in 2007. These drugs included, among others, cannabis, sedatives, narcotics, stimulants and anti-depressant medications. As can be expected from recent legislative changes, the drug with the sharpest increase in use was cannabis. Drivers who tested positive for the drug leapt from 8.6 percent in 2007 to 12.6 percent in the 2013-2014 study.

The number of drug-impaired driver evaluations reported by Drug Recognition Experts also reflects this concerning trend. From 2009 to 2015, the number of formal drug influence evaluations reported by Drug Evaluation and Classification (DEC) Program state coordinators rose from 24,059 to 28,542, nearly a 20% increase. The number of DREs rose by only 6 percent during that time. Cannabis was the most frequently identified drug category in 2015, being identified in 10,880 DRE evaluations nationally – a 25 percent increase from 2012.

This data demonstrates an enormous and increasing need for law enforcement to expand their efforts to combat drug-impaired driving. Recent trends in cannabis legislation, and attempted cannabis legislation, suggest that the need for vigilance in this area will continue to increase in coming years.

Law Enforcement Countermeasures: Officer Training

Law enforcement managers should consider officer education the most fundamental step in effectively combating drug-impaired driving. NHTSA, in cooperation with the International Association of Chiefs of Police (IACP), maintains a series of progressive curriculum packages to build officer expertise in the area of alcohol

and drug impairment. The pinnacle of these programs is Drug Recognition Expert training.

Use of Drug Recognition Experts (DREs) is a vital component of any law enforcement response to the drug impaired driving issue. Simply put, a DRE is trained to make a three-point determination about suspected impaired drivers:

1. Is the driver impaired?
2. If the driver is impaired, is the impairment due to drugs or a medical condition?
3. If the impairment is drug-induced, what category or categories of drugs are causing the impairment?

The training to become a DRE is a rigorous process, but attainable for dedicated officers. It includes a two-day "DRE Preschool" that is designed to assess the candidate's ability to move forward in the program and prepare them for the next phase. Candidates who successfully complete the preschool then transition to a 7-day classroom phase where they learn the 12-step drug influence evaluation process, details of drug influence symptomatology, and how to execute the three-point determination described above. Upon passing the classroom phase, candidates then move onto a field certification phase in which they must conduct hands-on evaluations of actual drug impaired subjects and correctly render decisions about them. The final step in the certification process is then successful completion of the Final Knowledge Exam, which includes a detailed exploration of the knowledge they gained through the entire process up to that point. More details about the process and how it is supported in each state can be obtained from the state's DRE State Coordinator.

Law enforcement managers must understand that the value of DREs extends well beyond arrests they personally make. DREs supplement and bolster the arrests of other officers, provide expert testimony on cases made by other officers, and can serve as a community resource in a variety of contexts. Despite their great value, DREs only compose a small percentage of the law enforcement officers nationally.

According to the IACP, which manages the credentialing process for DREs, there were approximately 8,000 DREs, spread across 3,681 agencies, in the United States on December 31, 2016. The program is also represented in Canada, the United Kingdom, China, and Germany.

To aid in bridging the gap between the basic training received by most police officers in DUI Detection & Standardized Field Sobriety Testing and DRE training, NHTSA and IACP developed Advanced Roadside Impaired Driving Enforcement (ARIDE). ARIDE solidifies the student's proficiency in Standardized Field Sobriety Tests, trains them to administer two additional examinations, introduces the concepts of pupil size change as an indicator of drug influence, and familiarizes candidates with foundational concepts in identifying drivers under the influence of drugs other than alcohol. The standard ARIDE course is a 16-hour class available in all 50 states.

According to statistics from NHTSA's national tracking system for DRE Drug Influence Evaluations, ARIDE has proven to be a successful tool for screening impaired drivers into DRE evaluations for many states. For example, the tracking system indicates that 50.6 percent of the DRE enforcement evaluations conducted in Washington State during 2015 resulted from an impaired driving arrest made by an ARIDE-trained officer.

For more information about ARIDE and DRE training, as well as assistance contacting a DRE State Coordinator, visit www.decp.org

Law Enforcement Countermeasures: Refusal of Chemical Testing

Even when well-trained officers develop a strong body of evidence against an impaired driver using standardized sobriety testing, the lack of chemical testing can be a serious challenge to obtaining convictions in court. While there does not seem to be a credible estimate of blood draw refusals in recent years, research indicates that the average refusal rate for breath tests in 2011 was 24 percent (median 18 percent) across 34 states for which data was available. [2]

Several states in the United States have statutes allowing police officers to obtain search warrants for blood in the case of an impaired driver that refuses the state chemical test. The Arizona Department of Public Safety (AZDPS) was one of the first law enforcement agencies to implement large-scale use of search warrants and "no refusal" programs on impaired driving cases, and they can be considered a model for other agencies interested in aggressively combating this issue. AZDPS troopers apply for search warrants electronically when a driver refuses chemical testing and are able to execute the blood collection with little delay.

With the frequent use of search warrants for blood in their agency, AZDPS has also implemented a law enforcement phlebotomy (blood drawing) program to reduce complications and delays involved with using a third-party for sample collection. Troopers attend a 40-hour course for initial phlebotomy certification, then maintain the certification through meeting certain ongoing requirements. The ability to eliminate wait times at hospitals or other medical facilities is of particular

importance with drivers under the influence of cannabis, as research shows that THC blood concentration decreases an average of 73.5 percent in the first half-hour and 90.3 percent in the first 1.4 hours after smoking. [3] The ability of officers to draw samples themselves improves their collection time, as compared to the generally accepted 1.5 – 4-hour average range to obtain a blood sample using third-party personnel. For more information on other considerations in law enforcement phlebotomy programs and how to go about establishing a similar program in your state, contact the Arizona Law Enforcement Phlebotomy Program Coordinator via the Arizona Governor's Office of Highway Safety.

Challenges and Recommendations: Chemical Testing Policy and Practice

The observations and clearly articulated opinions of a well-trained officer should serve as the foundation for any impaired driving case, but chemical testing provides a useful, and sometimes crucial, means to support the officer's findings of impairment.

Even when a biological sample is collected by law enforcement for analysis, the content and scope of testing may still vary significantly between states. For example, some state statutes only allow law enforcement to collect urine for chemical testing purposes. This restricts the usefulness of the test in proving impairment, since urine shows historical (not necessarily recent) use of a drug and cannot be easily correlated to a level in the blood (where it can affect driving). In the case of such statutes, law enforcement managers should work with their state officials to move towards legislation more supportive of convicting impaired driving cases. A more common point of variance between states is the scope of drugs tested for and the minimum levels at which their lab can confirm and quantify the presence of a drug. Even with the longstanding record of cannabis as the most abused illicit drug in the United States, [4] some labs still do not test and confirm the presence of THC in blood - only an inactive metabolite. Others may confirm THC, but only at levels notably higher than where some people may be impaired. Similar issues extend to other drugs, both licit and illicit. Not only is this a challenge to convicting impaired drivers, but it may create the false impression of officers making unjustified arrests. In 2016, the International Association of Chiefs of Police (IACP) joined the National Safety Council's Alcohol, Drugs, and Impairment Division (NSC ADID) in supporting recommendations set forth in "Recommendations for Toxicological Investigation of Drug-Impaired Driving and Motor Vehicle Fatalities," [5] which provides recommendations for confirmation levels and scope of testing for forensic toxicology laboratories. The IACP's resolution encourages law enforcement to work in partnership with their toxicology labs to support implementation of the recommended standards. This resolution, and others, can be reviewed at http://www.theiacp.org/Resolutions.

With the expansion of medical and recreational cannabis laws across the country, several states have current or pending legislation that sets a *per se* threshold (other than zero) for THC in the blood. While the intent of such laws is typically to create a presumption of impairment over a certain level, the practical implication of such laws is often that attorneys and jurors erroneously presume drivers *under* that limit are *not* impaired. A recent position paper from the NSC ADID cautions that "It is further concluded that due to rapid changes in blood THC concentrations over time, there is no minimum safe threshold blood concentration below which a driver can be considered to have been unaffected while driving following recent cannabis use. Consequently there is no scientific basis for the adoption of THC *per se* laws for driving." Law enforcement managers should consider the challenges described in this position paper, and bring them to the attention of lawmakers when matters related to cannabis legalization or *per se* laws are at issue. [6]

The proliferation of drug-impaired driving has cued development of additional roadside testing technology that may assist officers with confirming the presence of certain drugs in a biological specimen, similar to portable breath testing devices used in alcohol cases. The most promising developments in this area are related to oral fluid testing. A small number of states are currently running pilot programs to test the practicality and reliability of roadside oral fluid testing. If this technology proves to have valid applications in roadside impaired driving enforcement, many states will still face hurdles due to state laws that prohibit such testing or require that a state agency endorse any device to be used for chemical testing. Current research correlating levels of a drug in oral fluid to levels in blood is also critically lacking, so early adoption of this technology will likely only be useful for establishing presence of the drug.

Public Education

NHTSA's Fatality Analysis Reporting System (FARS) indicates a reduction of over 50 percent in the number of traffic deaths attributable to alcohol-impaired driving between 1982 and 2014. While law enforcement efforts to deter impaired driving and apprehend violators have been important contributors to this decline, so too have public education campaigns implemented by state and federal government agencies, as well as private entities such as Mothers Against Drunk Driving (MADD). Similar efforts on the topic of drug-impaired driving, particularly cannabis-

impaired driving, may be warranted as legislative and social trends continue to facilitate increasing numbers of people likely to operate a vehicle while impaired by drugs. Jurisdictions newly facing the issue of increased cannabis-impaired driving can look to states like Colorado that have spent years developing programs specifically targeting that problem. The Colorado Department of Transportation (CDOT) has launched campaigns like "Drive High, Get a DUI", staged clever public demonstrations to draw the attention of the general public and recreational marijuana users, installed video games with sober driving messages at dispensaries to engage marijuana users at point of sale, and even partnered with ride-sharing services to increase awareness of safe ride alternatives. Countermeasures like these hold great promise in minimizing traffic fatalities related to drug impaired driving.

Notes:

1. National Highway Traffic Safety Administration. Results of the 2013-2014 National Roadside Study of Alcohol and Drug Use by Drivers. By A. Berning, R. Compton, and K. Wochinger. Washington, D.C.: National Highway Traffic Safety Administration, 2015.
2. Jones, R. K., and James L. Nichols. Breath test refusals & their effect on DWI prosecutions. Washington, D.C.: U.S. Dept. of Transportation, National Highway Traffic Safety Administration, 2012.
3. Hartman, R. L., T. L. Brown, G. Milavetz, A. Spurgin, D. A. Gorelick, G. R. Gaffney, and M. A. Huestis. "Effect of Blood Collection Time on Measured 9-Tetrahydrocannabinol Concentrations: Implications for Driving Interpretation and Drug Policy." Clinical Chemistry 62, no. 2 (2016): 367-77. doi:10.1373/clinchem.2015.248492.
4. Center for Behavioral Health Statistics and Quality. (2015). Behavioral health trends in the United States: Results from the 2014 National Survey on Drug Use and Health (HHS Publication No. SMA 15-4927, NSDUH Series H-50). Retreived from http://www.samhsa.gov/data/sites/default/files/NSDUH-FRR1-2014/NSDUH-FRR1-2014.pdf
5. Logan, B. K., K. J. Lowrie, J. L. Turri, J. K. Yeakel, J. F. Limoges, A. K. Miles, C. E. Scarneo, S. Kerrigan, and L. J. Farrell. "Recommendations for Toxicological Investigation of Drug-Impaired Driving and Motor Vehicle Fatalities." Journal of Analytical Toxicology 37, no. 8 (2013): 552-58. doi:10.1093/jat/bkt059.
6. Position on the Use of Cannabis (Marijuana) and Driving. February 12, 2017. Position Paper of the National Safety Council's Alcohol, Drugs and Impairment Division

Contributor Acknowledgements

Chuck Hayes, DECP Project Manager, International Association of Chiefs of Police

Capt. Tim Mason, Arizona Department of Public Safety

Lt. Ron Kessler and Lt Rob Sharpe, Washington State Patrol

Glen Beck, Highway Safety Program Manager, Colorado Department of Transportation

Amy Miles, Forensic toxicology Section Director, Wisconsin State Laboratory of Hygiene

Distracted Driving

Distracted driving has emerged as a significant problem that requires the resources of law enforcement agencies. In some jurisdictions, distracted driving now exceeds alcohol as a contributing factor in crashes. Law enforcement agencies face the reality that nearly 68 percent of U.S. adults now own a smartphone. At any given moment during the daytime, more than 800,000 vehicles are being driven by an individual who is using a hand-held cellphone. [1]

Lawmakers have responded with primary laws banning texting while driving and youth under the age of 18 from using a cell phone while driving. There has also been legislation passed that requires distracted driving issues to be included in the state driver's license examination. As of April 2019, 48 U.S. states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have banned text messaging for all drivers, while all but 3 states have primary enforcement laws. [2]

NHTSA's "Road to Zero Fatalities" campaign and Strategic Plan address human factors as the primary causes of crashes, including impaired, drugged, distracted, and drowsy driving. NHTSA has emphasized the importance of these issues in a concerted education and awareness campaign. Law enforcement leaders are encouraged to review NHTSA's Distraction.gov website (https://www.distraction.gov/index.html) for links to best practices and campaigns conducted by law enforcement agencies to address the issue of distracted driving. [3]

The New York State Police (NYSP) and the Dalton, Georgia, Police Department (DPD) offer two innovative approaches to distracted driving. The NYSP model consists of a multi-pronged strategy emphasizing executive leadership starting with the governor of New York; data analysis; problem identification; public information and education, particularly with programs focused on youths; and enforcement. For their efforts in 2015, the NYSP was selected as the winner of the Distracted Driving Special Award winner in the 2016 National Law Enforcement Challenge (NLEC). Several important lessons learned by the NYSP in addressing this traffic safety issue could assist other agencies in replicating their success:

- **Lead with leadership:** Moving the needle on distracted driving requires strategic support at the highest levels, both internally and externally. One example of this was New York Governor Andrew Cuomo's creation of 91 "Texting Zones," where motorists can safely pull over on a roadway to use their mobile phones. The priorities of the command staff resonate agency-wide.

- **Stories sway:** Victim-impact stories can help change driver behavior by highlighting the human cost of distracted driving crashes.
- **Stealth drives success:** Covert SUVs have a significant tactical advantage over marked patrol cars during distracted driving enforcement due in part to their higher stance relative to other cars. [4]

The winner of the Distracted Driving Special Award in the 2015 NLEC, the DPD zeroed in on the issue in 2014 by focusing on specialized training, targeted education, and concentrated enforcement. With a population of 33,000 citizens and 61 sworn officers, community surveys revealed distracted driving as a top citizen concern. During a roadside visual survey, the DPD found that over half of observed motorists were engaged in some type of distracted behavior while operating their vehicles. Leadership in the DPD selected the month of October to be dubbed "Distractober," with correlating "Operation Thumbs Up/Distractober" campaign initiatives that included problem identification using community surveys, education of officers and citizens, and selective traffic enforcement details. The DPD reported a 23.7 percent reduction in distraction-related crashes following these efforts. Other lessons learned included:

- **Community input is important:** Citizen surveys can help agencies identify critical traffic safety issues.
- **Limited campaigns can produce lasting results:** Organized, short-term education and enforcement campaigns can help agencies target specific traffic problems in a meaningful way.
- **Enforcement yields education:** Traffic stops are an excellent opportunity to educate drivers on the hazards of distracted driving as well as enforce the law. [5]

To learn more about distracted driving initiatives, refer to the IACP website: https://www.theiacp.org/topics/traffic-safety

Notes:

1. National Conference of State Legislatures, "Distracted Driving," March 3, 2016, accessed February 3, 2017, http://www.ncsl.org/research/transportation/spotlight-distracted-driving.aspx.
2. "Distracted Driving," Governors Highway Safety Association, accessed June 7, 2019, https://www.ghsa.org/index.php/state-laws/issues/distracted%20driving.
3. "Distracted Driving," National Highway Traffic Safety Administration, accessed February 3, 2017, https://www.distraction.gov/index.html.
4. "Dialing Against Distractions," *Traffic Safety Innovations 2016* (IACP, 2017), accessed February 22, 2017, http://www.theiacp.org/Portals/0/documents/NLEC/Distracted%20Driving_v1.pdf.
5. "A Serious Distraction," *Traffic Safety Innovations 2015* (IACP, 2016), accessed February 3, 2017, http://www.iacp.org/Portals/0/documents/NLEC/Distracted%20Driving.pdf.

Drowsy Driving

Drowsy driving is not simply falling asleep at the wheel; it is a profound impairment that mimics alcohol-impaired driving in many ways. Drowsiness leads to slower reaction times and impaired attention, mental processing, judgment, and decision-making. Drowsiness can occur from accumulating sleep debt, typically less than six hours per night across multiple nights, or from only one night of not sleeping. Precise statistics of crashes caused by drowsy driving are not yet possible. Crash investigators can look for certain clues that indicate drowsiness was a likely contributor to driver error, but these clues are not always identifiable or conclusive. In lieu of consistent and conclusive evidence, researchers have used various methods to estimate the overall number of crashes or crash fatalities caused by driver drowsiness. [1]

NHTSA developed the "Drowsy Driving Research and Program Plan" in order to address the problem of drowsy driving in the United States. This plan has six broad focus areas, including measurement and problem identification, public awareness and education, policy development, high-risk populations, vehicle technology, and infrastructure. There will be a total of ten projects initiated with emphasis on these focus areas to enhance the science and program initiatives around drowsy driving. [2]

GHSA's "Wake Up Call! Understanding Drowsy Driving and What States Can Do" campaign is an important initiative that provides law enforcement agencies with excellent resources on this issue, such as a recorded webinar and a unique report examining the causes and effects of drowsy driving. The report contains adaptable best practices from agencies in Iowa, Utah, Texas, and New York to address drowsy driving. More information and resources can be found on the campaign's website: http://www.ghsa.org/resources/wake-call-understanding-drowsy-driving-and-what-states-can-do. [3]

Addressing the problem of drowsy driving is essential and the task is even more complex due to the following:

- The true extent of the problem is hampered by incomplete data;
- There is limited objective data to determine if a motorist is too tired to drive; and
- The general public does not fully understand the importance and dynamics of sleep and its impact upon safe driving. [4]

An important point has been established based upon research studying the similarities between drowsy driving and impaired driving. The Centers for Disease Control and Prevention (CDC) published an article which discussed

studies demonstrating how the lack of sleep mimics impairment and the ability to safely operate a motor vehicle. The CDC reported that being awake for at least 18 hours is the same as someone having BAC of 0.05 while being awake for at least 24 hours is the equivalent to have a BAC of 0.10. [5]

Working together with NHTSA, SHSOs, and other key partners, law enforcement can make drowsy driving a year-round priority. Potential specific strategies include:

1. Participating in the National Sleep Foundation's (NSF) Drowsy Driving Prevention Week each November. Law enforcement can work collaboratively with community partners to raise awareness and conduct enforcement efforts.

2. Educating themselves about the dangers of drowsy driving and being alert to the signs of drivers who may be under the influence of medications in order to help them stay awake on the roads. This may involve a partnership with their state's commercial vehicle enforcement units and DRE-trained officers who may have more advanced training and techniques to detect drowsy driving.

3. Leading or forming key partnerships during campaigns to educate shift workers, commercial vehicle operators, and adolescents on the dangers of drowsy driving. Educational materials are available from organizations like NSF, NHTSA, GHSA, and FMCSA.

4. Analyzing crash data with an emphasis on known drowsing driving high-risk corridors. Law enforcement officers can then conduct patrols where they are alert to the cues and behavioral signs of drowsy driving. Advertising these data-driven efforts, coupled with high-visibility enforcement, to address drowsy driving may have a deterrent effect.

5. Encouraging law enforcement leaders to contact their SHSO to learn more about best practices, funding for drowsy driving initiatives, and the latest research.

Notes:

1. Namni Goel et al., "Neurocognitive Consequences of Sleep Deprivation," *Seminars in Neurology* 29, no. 04 (2009): 320–39, accessed February 3, 2017, doi:10.1055/s-0029-1237117, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/drowsydriving_strategicplan_030316.pdf.
2. Ibid.
3. "Wake up Call! Understanding Drowsy Driving and What States Can Do," *Governors Highway Safety Association,* 2016, accessed February 3, 2017, http://www.ghsa.org/resources/wake-call-understanding-drowsy-driving-and-what-states-can-do.
4. "WAKE UP CALL! Understanding Drowsy Driving and What States Can Do," *Governors Highway Safety Association,* 2017, http://www.ghsa.org/sites/default/files/2017-02/Drowsy%202016-U.pdf.
5. "Drowsy Driving," *Centers for Disease Control and Prevention,* February 18, 2016, accessed February 16, 2017, https://www.cdc.gov/sleep/about_sleep/drowsy_driving.html.

Aggressive Driving

Aggressive driving, according to NHTSA, is when individuals commit a combination of moving traffic offenses, and in doing so, endanger other persons or property. Driving behaviors that commonly constitute aggressive driving include speeding, racing, frequently changing lanes, cutting off other drivers, failing to signal, running red lights, failing to yield, tailgating, slowing rapidly to discourage a tailgater, boxing in other vehicles, and using other intimidation maneuvers. [1]

The problem of aggressive driving can be further compounded by overt acts of intimidation such as gesturing or shouting at other operators. In some extreme cases, aggressive drivers have even reportedly engaged in assaultive and menacing behaviors towards other motorists, sometimes even using a firearm. Factors that lead to aggressive driving include road construction, extreme traffic congestion, perceived bad driving, and a general lack of patience in society today. [2]

States have addressed aggressive driving legislatively in different ways. Some have defined aggressive driving as a separate offense, while others may group it under the reckless driving statute. Generally, aggressive driving includes the behaviors often covered under the reckless driving law. However, other states have added language that defines a pattern of behaviors occurring over a short period with or without intention. States with a statute that require intention often find this difficult to prove, and thus use their reckless driving statute to cite offenders. The definition of aggressive driving often includes that these driving behaviors could result from aggression, selfishness, or competition. Many of the behaviors that constitute aggressive driving could also occur in the absence of aggression; for example, if a driver is inattentive. Several state legislatures use a threshold of three or more potentially aggressive behaviors committed in a sequence or over a short period of time in their statutory definitions of aggressive driving.

Aggressive driving may lead to more extreme actions on the part of the offender known as "road rage." This may involve criminal intimidation, sometimes coupled with violence, precipitated by driving activities. Road rage involves an intent to harm and can involve the use of the vehicle as a weapon take place outside the vehicle(s) involved. [3]

Response Strategies

A multi-disciplined approach to aggressive driving involving enforcement, legislation, environmental and situational factors, public education, and judicial responses are viewed as most effective. Law enforcement agencies

that use a blend of comprehensive strategies may see the most success in impacting aggressive driving behaviors. By using data to identify and then target known aggressive driving high-risk corridors, law enforcement can be most effective in addressing this issue. Other effective strategies include enforcement and sanctions to target individual aggressive drivers. Additionally, a focus on the driving environments, public education and awareness, and situational stressors that lead to aggressive driving, such as road construction during peak commuting hours, are suggested. [4]

Traffic enforcement to address aggressive driving has three primary goals:

- Deter cited drivers from driving aggressively in the future;
- Deter other drivers who learn about police enforcement from driving aggressively; and
- Remove aggressive drivers from the roads while they are angry and most dangerous.

Deterrence is advanced through significant fines or other consequences such as jail time, and through high-visibility enforcement. Effective enforcement campaigns typically include an emphasis on public information and education strategies, including roadside warnings. [5]

Best Practices in Targeting Aggressive Driving

A NHTSA-sponsored study entitled "Aggressive Driving Enforcement: Evaluation of Two Demonstration Programs" assessed the effects of two programs that were implemented to reduce the incidence of aggressive driving. The programs were conducted by the Marion County Traffic Safety Partnership a consortium of agencies in the vicinity of Indianapolis, Indiana, and the Tucson, Arizona, Police Department. Study results suggested that limited resources might be best spent on officer enforcement efforts, as opposed to public awareness campaigns. The study also found assigning full-time enforcement responsibility to a small team of officers to conduct special enforcement patrols may be more effective than tasking a larger number officers with an occasional overtime duty. The study also showed that crashes caused by aggressive driving can be effectively deterred by a combination of enforcement and public information and education.

Notes:

1. Colleen Laing, "Aggressive Driving," Center for Problem-Oriented Policing, Guide No. 16 (2010), http://www.popcenter.org/problems/aggressive_driving/.
2. Ibid. Laing.
3. "Statutes & Constitution: View Statutes: Online Sunshine," Florida Legislature, 1995, accessed February 16, 2017, http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0300-0399/0316/Sections/0316.1923.html.
4. Ibid. Laing.
5. Ibid. Laing.

Young Drivers

The Insurance Institute for Highway Safety (IIHS) reports that teenage drivers have the highest crash risk per mile traveled, compared with drivers in other age groups. The challenge for youths operating a motor vehicle is their over-confidence in their driving skills and a failure to perceive the many hazards that exist on the road. [1] A 2014 study published in the *New England Journal of Medicine* demonstrated that one of the riskiest driving behaviors is the performance of secondary tasks requiring drivers to look away from the road, and that novice drivers appear to be especially prone to this type of activity while dialing or texting on a smartphone. [2] This kind of risky driving behavior is often compounded by the likelihood that other factors, such as inexperience, lack of awareness of risks, and speeding, are more common factors with novice drivers.

All 50 states in the U.S. and the District of Columbia have a three-stage Graduated Driver Licensing (GDL) system. GDL licensing has reduced teen crashes between 10-30 percent on average. Generally, these stages are:

1. The Learner Stage, which allows novice drivers the opportunity to drive under supervised conditions (typically with an adult).
2. The Intermediate Stage, which provides driving practice under restricted conditions prior to obtaining a full license. Restrictions may include number of passengers, minimum age, etc.
3. The Unrestricted Stage, which outlines when nighttime and passenger restrictions may be rescinded. [3]

GDL laws can be complex, but it is imperative that law enforcement officers are intimately familiar with their provisions. Law enforcement executives are encouraged to ensure their officers are aware of the importance of the GDL laws in their jurisdiction. GHSA is one organization that has encouraged law enforcement leaders to be aware of the risks for teen drivers and to understand the way GDL laws can help reduce these risks. Some effective strategies that law enforcement can lead include special awareness and education campaigns, targeted enforcement, and partnerships with community organizations and schools.

GHSA has found the following key take-aways are important for law enforcement to ensure success with their efforts:

1. Use peer-to-peer training initiatives to educate command staff about the risks for teens and how GDL works to address those risks.
2. Establish formal standard operating procedures (SOPs) for managing teens cited for passenger and nighttime driving violations.
3. Ensure that teen drivers fully understand the seriousness of GDL violations and ensure this information is shared with their parents.
4. Recognize that initial enforcement of GDL laws can present challenges. GDL laws can be complex and difficult for officers to fully understand. Training on GDL laws is essential for law enforcement.
5. A public awareness campaign, such as a voluntary GDL decal program to designate a GDL holder, is one way to raise awareness and garner the support of parents and the public. One example is a voluntary "Novice Driver" magnet that is provided to all GDL holders in the State of Delaware. [4]

NHTSA convened a Teen Driver Focus Group which studied teen driving behaviors. The focus group provided feedback on a variety of key topics and these are summarized as follows:

- **Enforcement:** Some teens reported an ability to avoid getting a ticket for GDL or traffic violations. Teens reported a deterrent effect when the certainty of being cited was high, as this could impact their ability to have full driving privileges.
- **Occupant protection:** Teens are well-aware of campaigns such as *Click It Or Ticket* and the importance of seatbelts.
- **Speeding and aggressive driving:** Focus group participants did not think driving five or ten miles over the posted speed limit was dangerous.
- **Distracted and drowsy driving:** Participants failed to see the link between these dangerous behaviors and the high rate of crashes. The prevalence of smartphones in this demographic group compounds the issue of distracted driving.

This study highlights general trends on key areas, and more information is needed to determine the relationship between teen unsafe driving and the rate of crashes. [5]

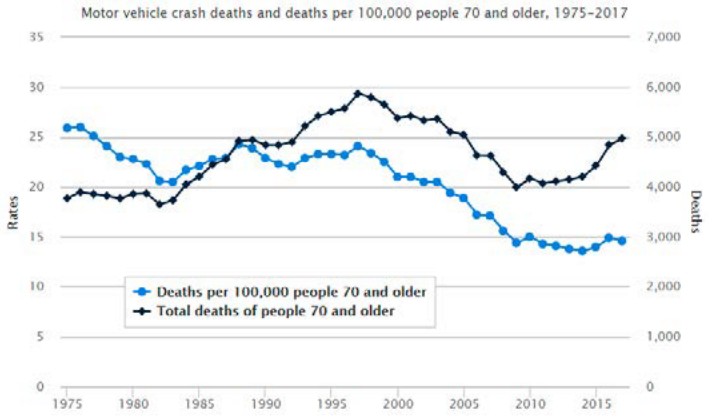
The combination of GDL programs and proactive enforcement of existing GDL laws will help address the risks of teen driving. Law enforcement leaders are encouraged to combine this approach with parent and teen engagement, using traffic stops as an educational opportunity, as well as targeted media coverage to help raise greater awareness and promote safe teen driving in their communities.

Notes:

1. "Licensing Systems for Young Drivers," *Insurance Institute for Highway Safety,* 1612, accessed February 6, 2017, http://www.iihs.org/iihs/topics/laws/graduatedlicenseintro?topicName=teenagers.
2. Sheila G. Klauer et al., "Distracted Driving and Risk of Road Crashes Among Novice and Experienced Drivers," *New England Journal of Medicine* 370, no. 1 (January 2, 2014), doi:10.1056/nejmsa1204142.
3. "Licensing Systems for Young Drivers," *Insurance Institute for Highway Safety,* 1612, accessed February 6, 2017, http://www.iihs.org/iihs/topics/laws/graduatedlicenseintro?topicName=teenagers.
4. "Curbing Teen Driver Crashes," *Governors Highway Safety Association,* 2012. http://ghsa.madwolf.com/html/files/pubs/sfteens12.pdf.
5. "Teen Unsafe Driving Behaviors: Focus Group," *Traffic Safety Facts* (NHTSA 2006), https://permanent.access.gpo.gov/lps102414/tt318.pdf.

Older Drivers

NHTSA and the IIHS have studied important trends regarding older drivers. While some recent data points to a reduction in the total number of fatal collisions, almost 5,000 people over the age of 70 died in car crashes in the United States in 2017. This total is 15 percent less than the total in 1997, but a 32 percent increase since 1975. While this data reflects an improvement, there is still much work to be accomplished, especially since seniors represent the fastest-growing segment of drivers. [1]



[2]

The IIHS reports that the number of drivers over the age of 70 is growing, and, with baby boomers maturing, seniors now make up a higher proportion of the population in the U.S. Older drivers are more active and have a tendency to keep their driver's licenses longer, as well as drive more miles than previous senior generations. Per miles traveled, fatal crash rates increase significantly between the ages of 70-74 and climb to their highest rates for drivers 85 and older. These increases are attributed to elevated

injury susceptibility, particularly chest injuries and medical complications, rather than an increased tendency be involved in crashes. [3]

The AAA Foundation for Traffic Safety is another organization that can provide excellent resources and maintains the website "SeniorDriving.AAA.com" (http://seniordriving.aaa.com/). This website is an exceptional informational tool for law enforcement leaders to consult when considering new initiatives to address the complexities of senior drivers. There are free downloads and assessments that officers can share with seniors in their communities. [4]

The AAA Foundation also shared research on senior drivers and causation factors related to these motorists and crashes. There are three key functions that law enforcement should be aware of when interacting with the older driver:

1. **Vision:** Adequate visual acuity and field of vision are critical for safe driving, but tend to decline with age.
2. **Cognition:** Driving requires a variety of high-level cognitive skill, including memory, visual processing, attention, and decision-making skills. Certain medical conditions, such as dementia, as well as prescription medication can have an impact on cognition in seniors.
3. **Motor function:** Motor abilities are necessary to enter a vehicle safely, fasten a seatbelt, turn to view approaching traffic, and operate vehicle controls. These motor abilities tend to decline as individuals age, and they can decrease an individual's ability to drive safely. [5]

Law enforcement officers have an important role in ensuring senior drivers are operating in a safe manner and not creating an unnecessary risk to other motorists. According to NHTSA, there are several effective strategies that law enforcement can implement in their communities to improve the safety of older drivers. Similar to other effective campaigns to address a special traffic safety problem or special population, there must be a combination of efforts that include enforcement, education, and outreach.

A law enforcement agency should consider partnering with one of many other nonprofit or community organizations to share data and educational materials with seniors on the primary causation factors of crashes involving this driving population. An excellent program entitled "Older Driver Law Enforcement Instructor Training" is sponsored by the International Association of Directors of Law Enforcement Standards and Training (IADLEST) and is held through a partnership with NHTSA. In this course, law enforcement officers learn effective strategies for addressing senior drivers, develop effective enforcement initiatives, and create new opportunities to improve community relations related to the senior driving population. [6]

Other effective proactive steps that law enforcement officers can take include the following:

- Analyze and study location data and the incidence of crashes that involve elderly drivers, and work closely with state highway engineers to evaluate the need for changes in traffic control devices, warning signs, and traffic patterns. This can be especially important in known areas of high concentrations of senior citizens.
- Identify drivers with potential driving impairments and refer them to the state Division of Motor Vehicles for follow-up testing.
- Ensure that older drivers who are stopped for motor vehicle violations are not allowed to proceed with only verbal warnings, when younger drivers would receive citations. This negates the lifesaving benefits of the point system to detect individuals who commit particularly serious violations or violate traffic laws on multiple occasions.
- Be alert to drivers who appear to be lost or confused; stop them and inquire as to their welfare. If a driver appears to be suffering from some form of dementia, the motorist should not be allowed to proceed farther; instead, the individual should be referred to the motor vehicle licensing authority for reexamination and should have relatives or next-of-kin contacted to advise them of the situation.
- Make sure that officers receive periodic training in elderly issues, including the ability to recognize dementia and interact properly and sensitively with drivers who may be suffering from debilitating diseases, such as Alzheimer's. Local chapters of the Alzheimer's Foundation are always willing to participate in such training and provide police with tools and resources to raise their awareness. [7] For more information, refer to the NHTSA website: https://www.nhtsa.gov/road-safety/older-drivers

Law enforcement agencies can also play an important educational role in preventing crashes involving elderly drivers. The American Association of Retired Persons (AARP) has a driver-training program developed especially for older drivers. This program can be presented by law enforcement officers, in partnership with senior citizen volunteer instructors, at senior citizen centers and senior social events. It teaches mature drivers how to recognize and overcome their infirmities, as well

as self-assess their own driving skills. Such programs can build rapport with an ever-increasing segment of the population while also providing a life-saving service.

Notes:

1. "Fatality Facts," *Insurance Institute for Highway Safety,* accessed February 7, 2017, http://www.iihs.org/iihs/topics/t/older-drivers/fatalityfacts/older-people#Trends.
2. Anne McCartt, "Q&As Fatality Facts State Laws News Releases and Articles Public Presentations Regulatory and Legislative Policy HLDI Research Selected IIHS Bibliography The Older Driver Crash Picture: Trends and Factors" (presentation, Lifesavers National Conference on Highway Safety Priorities, Chicago, Illinois, 2015).
3. Ibid. "Fatality Facts."
4. "Seniordriving.AAA.com," *AAA Senior Driving,* 2017, accessed February 7, 2017, http://seniordriving.aaa.com/.
5. "Mature Drivers," *Governors Highway Safety Association,* September 27, 2011, accessed February 7, 2017, http://www.ghsa.org/issues/mature-drivers.
6. "Older Driver Law Enforcement Instructor Training," *International Association of Directors of Law Enforcement Standards and Training,* 2017, accessed February 7, 2017, https://www.iadlest.org/Projects/OlderDriverLawEnforcementTraining.aspx.
7. *Highway Safety Desk Book* (n.p., 2004), 18-5 – 18-6, https://ntl.bts.gov/DOCS/deskbk.html.

Bicycle and Pedestrian Safety

Throughout the United States, there has been a pronounced increase in the number of citizens who are walking or cycling as their primary means of commuting to work. Whether it is to save on commuting and parking costs, for their own health and fitness or to have a reliable means of accessing public transportation, people want to take advantage of economical transportation options. Cycling and walking are not only lifestyle choices, they are a reality as communities take steps to promote safe and connected communities. The over-reliance upon the motor vehicle as the sole option for commuting has been undergoing a positive shift. Several states and cities are actively promoting alternatives through proactive education and awareness initiatives.

As the number of pedestrians and cyclists on the roads increase, law enforcement officials will need to play an important role in ensuring that commuting options are safe. The increase in fatality percentages are show in the graph below. On average, pedestrians make up 15 percent of all traffic fatalities, while bicyclists make up approximately 2 percent. These rates have unfortunately been trending higher in recent years, despite a slight decrease of 1.7 percent from 2016 to 2017. [1]

According to GHSA, the rate of increase for those biking or walking has been significant as more citizens realize the many health, economic, environmental, and societal benefits of these options. Preliminary studies by the Federal Highway Administration (FHWA) and NHTSA point to the following contributing factors for the increase in pedestrian fatalities:

- Increased motor vehicle travel on all roads, perhaps due to the stabilization of fuel prices;
- Improved economic conditions;
- Increased opportunities for walking and biking;
- Increased interest in the health and fitness benefits attributed to walking and biking. [2]

Additional studies are being conducted; however, the following significant trends are seen when studying crashes involving pedestrians and cyclists:

- Increased use of cellphones and electronic devices are a source of distraction for drivers, cyclists, and pedestrians;
- Relationship between driver speed and severity of injury to cyclists and pedestrians;

Table 1
Occupants and Nonoccupants Killed in Traffic Crashes, 2016–2017

Description	2016	2017	Change	% Change
Total*	37,806	37,133	-673	-1.8%
Occupants				
Passenger Vehicles	23,877	23,551	-326	-1.4%
Passenger Cars	13,508	13,363	-145	-1.1%
Light Trucks	10,369	10,188	-181	-1.7%
Large Trucks	725	841	+116	+16.0%
Motorcycles	5,337	5,172	-165	-3.1%
Nonoccupants				
Pedestrians	6,080	5,977	-103	-1.7%
Pedalcyclists	852	783	-69	-8.1%
Other/Unknown	261	228	-33	—

Sources: Fatalities—FARS 2016 Final File, 2017 ARF
*Total includes occupants of buses and other/unknown occupants not shown in table.

- Use of roads between 6:00 p.m. and midnight leads to a pronounced risk of death; and
- Alcohol and drug impairment on the part of drivers, cyclists, and pedestrians increases the risk of crashes.

More data is needed, but the role of alcohol in pedestrian crashes is evident. NHTSA has estimated that alcohol use by either the driver or pedestrian is a contributing factor in 48 percent of pedestrian fatalities. [3]

The law enforcement response to fatalities involving pedestrians and cyclists needs to incorporate multi-pronged strategies. According to GHSA, several countermeasures seem to hold promise in efforts to reduce fatalities and injuries. The most effective strategies may require collaboration between law enforcement, SHSOs, transportation officials, and community leaders. The following approaches can be considered by law enforcement leaders for implementation in their communities:

- Increased separation between pedestrians, cyclists, and motor vehicles using refuge islands, sidewalks, bike paths, and overpasses, as well as new traffic signalization;
- Increased pedestrian and cyclist visibility by enhancing lighting;
- Addition of high-visibility crosswalks and rapid-flashing beacons mounted to pedestrian and cyclist crossing signs;
- Targeted traffic enforcement, including the use of automated enforcement technology;
- Public information and awareness campaigns;
- Educational outreach in high-risk areas; and
- Data analysis and mapping to identify high-risk zones. [4]

The July 2016 issue of *The Police Chief* magazine highlighted an effective program conducted in the State of Delaware, where fatalities accounted for approximately 25 percent of all crash-related deaths in the state. The Delaware Office of Highway Safety, Delaware State Police, Delaware Department of Transportation, and Christiana Care Emergency Services held a collaborative press event in November 2015 to draw attention to the issue of pedestrian fatalities. [5]

Part of this campaign was a two-week educational initiative that included the distribution of posters, postcards, and reflective flashlights at strategic locations, such as schools and community centers. Additionally, pedestrian safety messages and posters were disseminated using social media and placed in libraries, schools, and other public locations. The initiative also used data analysis to identify the location for the highest concentration of fatalities in the state.

A week-long enforcement effort followed the education and awareness component. The Delaware State Police used a combination of on-duty and overtime resources with funds made available by the SHSO, following the High-Visibility Education and Enforcement (HVEE) approach. HVEE offers an evidence-based, data-driven, problem solving strategy using proactive public education campaigns followed by targeted enforcement.

Following this campaign, representatives of the various agencies that participated in HVEE program met at IACP headquarters and discussed their individual HVEE strategies. Lessons learned in Delaware and the other participating states included:

- **Start with data:** Data is seen as critical to any successful HVEE campaign. NHTSA's FARS, combined with local agency data, can form the foundation for data analysis.
- **Starting small can be the best approach:** Participating agencies in Delaware focused on a three-mile stretch to address pedestrian fatalities. This was seen as a good way to start the campaign, which could be easily expanded into other high-risk corridors.
- **Identify partners:** Any initiative that is targeting traffic safety issues, including one that targets pedestrians or cyclists, should have both traditional and non-traditional partners and stakeholders supporting it.
- **Communicate:** As traffic safety campaigns progress, it is important to communicate both internally and externally to ensure that all participating partners understand the goals and objectives of the campaign.
- **Enhance enforcement with education:** Agencies can help build trust and understanding within their communities by focusing on the importance of safe practices, while simultaneously articulating the need for enforcement.
- **Keep the message fresh:** Continuous updates to the over-arching message are essential. Updates to social media, print media, and electronic communications are all important. The use of both traditional media and social media is also highly recommended.
- **Assess the campaign:** Continued assessment and evaluation of program goals and results will help determine where and when to allocate resources. [6]

The GHSA report *"Pedestrian Traffic Fatalities by State: 2017 Preliminary Data"* details state-specific examples of

safety initiatives and best practices. The Safe Routes to School program, administered by the University of North Carolina Highway Safety Research Center, is another excellent source of information on a host of pedestrian and cycling safety resources. NHTSA, FHWA, the IACP, and the CDC all offer helpful resources on their websites, which can be helpful to law enforcement leaders.

Recent trends show a likely increased use of non-motorized transportation options in the future. It makes good health and economic sense for individuals to take advantage of these options and for communities to expand these opportunities. It is important for law enforcement leaders to be aware of emerging trends, address problems, and respond with strategies that increase safety for all pedestrians and cyclists.

Notes:

1. "Research Note: 2017 Motor Vehicle Crashes: Overview," *Traffic Safety Facts* (NHTSA, August 2016), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812603.
2. Richard Retting, Heather Rothenberg, and Sam Schwartz Consulting, "2015 PRELIMINARY DATA Prepared for Governors Highway Safety Association" (GHSA, 2016), https://www.ghsa.org/sites/default/files/2018-03/pedestrians_18.pdf.
3. "Pedestrians," *Traffic Safety Facts,* (NHTSA, March 2018), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812493.
4. Ibid. Retting.
5. Brad Wentlandt, "High-Visibility Education and Enforcement (HVEE) Pilot Project," *The Police Chief* 83 (July 2016): 26–31, http://www.policechiefmagazine.org/high-visibility-education-and-enforcement-hvee-pilot-project/.
6. Ibid. Wentlandt.

Motorcycle Safety

The number of fatalities involving motorcyclists in the United States has recently decreased from a peak in 2008 of 5,112 deaths. A total of 5,172 motorcyclists died in crashes in 2017, a 10.2 percent increase from 2015. The data still show that fatalities have doubled since 1997 and continue to be an area of significant concern for NHTSA and law enforcement executives. [1] According to data from NHTSA, motorcyclists are 27 times as likely as passenger car occupants to die in a motor vehicle crash and 6 times as likely to be injured. [2]

As motorcycling has become more popular, especially over the course of the last 10 years, there has been a corresponding increase in crashes and fatalities involving motorcyclists. Motorcyclists accounted for a significant portion of the total number of motor vehicle fatalities. Despite the fact that motorcycles comprise only three percent of registered vehicles and less than one percent of vehicle miles traveled, they still account for nearly 15 percent of all motor vehicle fatalities. [3]

There are a number of contributing factors in many motorcycle crashes to include alcohol impairment, a significant increase in the number of registered motorcycles, lack of helmet use or use of novelty helmets (sometimes referred to as "brain buckets") that do not meet federal standards for crash protection, uneducated and unlicensed operators, and speeding. [4]

Using this data and additional ongoing research, NHTSA, GHSA, FHWA, and law enforcement executives have identified strategies to improve motorcycle safety. The most important findings include the need to ensure motorcycle riders are properly trained and licensed, the removal of alcohol-impaired operators from the roads, the need for all motorcyclists to wear Federal Motor Vehicle Safety Standard 218 helmets and clothing that provides both protection and visibility, the need to increase other motorists' awareness of motorcyclists by increasing visibility, and educating other drivers on the importance of sharing the road with motorcycles. [5]

IIHS reports that motorcycle helmet laws vary widely among states and there has been a considerable degree of change in the past fifty years. By the 1970's, almost all states had universal motorcycle helmet laws. However, in 1976, states lobbied Congress and new laws were adopted by states. This year marked the time when several states would no longer be assessed financial penalties for not having helmet laws. In 2019, 19 states and the District of Columbia have laws requiring all motorcyclists to wear a helmet, known as universal helmet laws. Laws requiring only some motorcyclists to wear a helmet exist in 28 states, while there are no helmet use laws in Illinois, Iowa, and New Hampshire. [6]

Best Practices in Addressing Motorcycle Fatalities

The New York State Police (NYSP) has been recognized by NHTSA and the IACP for a problem-based, comprehensive response to address fatal motorcycle crashes in the state. The NYSP approach to reducing motorcycle collisions and fatalities earned it the Motorcycle Safety Special Award in the 2016 National Law Enforcement Challenge (NLEC).

The NYSP found that motorcycles represented just over 3 percent of vehicle registrations on average in New York, however, they accounted for almost 15 percent of fatal crashes every year. Similar to national trends, the NYSP attributed the problem to helmets that did not meet federal standards, uneducated and unlicensed riders, and motorcycles that were in disrepair or lacked mandated safety equipment. The state police codified motorcycle safety and enforcement as a priority for the overall mission of the NYSP and enforcement details were increased, especially during the warmer months when ridership is at its highest levels. [7]

One of the key elements of the NYSP initiative was to begin focusing upon motorcycles the same way they approached commercial motor vehicles (CMV).

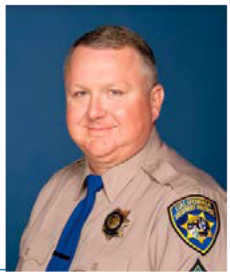
Motorcyclists were held accountable to a high standard of equipment and training compliance. A motor safety checkpoint program became a key component of the NYSP enforcement strategy. Troopers at the checkpoints check riders' licenses, helmets, and equipment, and the motorcycle is inspected for safety and noise compliance. The parallel approach to CMVs did not end with enforcement as officer education and experience was also addressed and improved upon. Troopers were offered additional training and familiarization with specialized laws related to motorcycles was also improved and eventually extended to local agencies and sheriff's departments. Additionally, motorcyclists were also offered additional educational materials while troopers also educated residents at public events across the state. [8]

The NYSP approach to motorcycle safety has had a significant impact, and fewer people are dying while operating a motorcycle. Following this initiative, the State of New York had a 6.7 percent decline in fatal motorcycle crashes, down from 164 fatalities in 2012 to 153 in 2015. [9] Through innovation, practical education, information, and enforcement, the NYSP has demonstrated how law enforcement officers can have a clear impact upon a challenging traffic safety problem.

Notes:

1. "Insurance Institute for Highway Safety," accessed February 19, 2017, http://www.iihs.org/iihs/topics/t/motorcycles/fatalityfacts/motorcycles#cite-text-0-0.
2. National Highway Traffic Safety Administration. 2016. Traffic safety facts, 2014: motorcycles. Report no. DOT HS-812-292. Washington, DC: US Department of Transportation.
3. "Motorcyclist Traffic Fatalities by State: 2015 Preliminary Data," 2016, accessed February 19, 2017, http://www.ghsa.org/resources/motorcyclist-traffic-fatalities-state-2015-preliminary-data.
4. Ibid. "Motorcyclist Traffic Fatalities by State: 2015 Preliminary Data."
5. *Traffic Tech: Countermeasures That Work, 8th Edition*, (n.p., 2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812239_countermeasures_8thed_tt.pdf.
6. Ibid. "Insurance Institute for Highway Safety."
7. *Traffic Safety Innovations 2016 Motorcycle Safety Shifting Safety Gears Treating Motorcycles Like Commercial Motor Vehicles Has Helped the New York State Police Reduce Reckless Driving*, (n.p., 2016), http://www.theiacp.org/Portals/0/documents/NLEC/Motorcycle%20Safety_v1.pdf.
8. Ibid. *Traffic Safety Innovations 2016 Motorcycle Safety Shifting Safety Gears Treating Motorcycles Like Commercial Motor Vehicles Has Helped the New York State Police Reduce Reckless Driving.*
9. Ibid. *Traffic Safety Innovations 2016 Motorcycle Safety Shifting Safety Gears Treating Motorcycles Like Commercial Motor Vehicles Has Helped the New York State Police Reduce Reckless Driving.*

Special Enforcement Initiatives to Reduce Crashes



By: **Sergeant Scott Taylor,** California Highway Patrol, Research and Planning Section

Adapted with permission from "Swarming Against Speeding," Traffic Safety Innovations 2016, The International Association of Chiefs of Police, (2016). Copyright held by the International Association of Chiefs of Police, 44 Canal Center Plaza, Suite 200, Alexandria, Virginia 22314 USA.

Swarming Against Speeding

Federal grants helped the California Highway Patrol reduce speed-related collisions with extra training, education, and enforcement.

California is well known for its pleasant weather, its diverse population, and its thriving industries, including entertainment, technology, and agriculture. From San Francisco to Los Angeles to San Diego, however, it is also well-known for its traffic jams, which are consistently ranked as among the nation's worst. In fact, Californians are so averse to congestion that they perpetually rush from point A to point B in a desperate attempt to circumvent it. The result, unfortunately, is a preponderance of speeding and aggressive driving that has come to characterize California roadways. To loosen speeding's grip on Golden State motorists, the California Highway Patrol (CHP) leveraged federal grant funding that allowed it to increase its investment in strategic anti-speeding solutions in 2015. How the CHP utilized these grants earned the agency the Speed Awareness Special Award in the 2016 National Law Enforcement Challenge (NLEC).

Problem Identification

A 2013 survey, conducted by the National Highway Traffic Safety Administration (NHTSA), found that nearly half of American drivers think speeding is a problem on U.S. roadways, and that an overwhelming majority of drivers (91 percent) think everyone should obey speed limits. However, one in five drivers admits, "I try to get where I am going as fast as I can," and more than a quarter say, "speeding is something I do without thinking" and "I enjoy the feeling of driving fast."

According to the CHP, these contradictions are lethal in California. In 2015, it reported 288 fatal traffic collisions and 30,747 injury traffic collisions in which speed was the

primary collision factor, making "unsafe speed for roadway conditions" the leading cause of California car crashes.

"Speeding is the number one contributor to collisions in California," says Sergeant Scott Taylor. "That makes it our prime target."

Planning

Although speeding is the CHP's prime target at any time of day, the agency's resources pale in comparison to the problem's size. To build more muscle with which to match speeding's strength, the CHP sought and received several federal traffic safety grants that allowed it to successfully scale its efforts in 2016.

The most significant of these grants, according to Taylor, was the statewide Reduce Aggressive Driving Incidents and Tactically Enforce Speed IV (RADIATES IV) grant. Awarded by the California Office of Traffic Safety (OTS) with funding through NHTSA, RADIATES IV provided resources that CHP divided amongst three strategic objectives: targeted statewide enforcement on state and federal roadway segments within the CHP's jurisdiction, division-selected roadway enforcement on state highways and county roads, and traffic safety presentations.

Beyond the grant, the CHP facilitated officer training and technology procurement. Specifically, the agency is continually training officers in radar and lidar-based enforcement, while constantly evaluating, repairing, and replacing its radar and lidar inventory.

"That's training our officers don't get at the police academy," explains Taylor, who says radar and lidar training give officers an opportunity to mature and refine their speed enforcement skills by learning how to use the latest speed enforcement technology and techniques.

The CHP also applied for and received two Area-wide regional traffic safety grants, again awarded by OTS with funding through NHTSA. Targeting two Areas with higher-than-average fatality and injury rates from speed-related traffic collisions, Ukiah and Central Los Angeles, the grants helped the CHP direct extra resources towards education and enforcement in communities statistically shown to need them.

Education

Public education and information was a key component of both the RADIATES IV and Area-wide regional traffic safety grants. For the former, efforts included press releases to local and statewide media outlets, a freeway billboard, and educational materials and banners distributed at various community events statewide, all of which contained anti-speeding messages. Additionally, the CHP conducted 706 traffic safety presentations highlighting the dangers of speeding and aggressive driving. Delivered at high schools, state fairs, and even baseball games, these presentations reached more than 156,000 people across California.

The CHP utilized the same public education strategies in its Ukiah and Central Los Angeles Area offices as part of its Area-wide regional traffic safety grants, but tailored them for local populations with the help of multijurisdictional task forces consisting of diverse community stakeholders, including the CHP, California Department of Transportation, legislature, courts, probation departments, health departments, public interest associations, and other organizations and individuals interested in improving traffic safety. The Ukiah Area office, for instance, installed traffic safety signs on a major state highway at four high-collision locations, gave traffic safety presentations, and distributed grant-funded educational materials at public events including, local fairs, Indian casinos, high school and college career fairs, health and safety fairs, child safety seat classes, and teen driver training classes. At the same types of venues, the Central Los Angeles Area office distributed brochures and posters in both English and Spanish in order to reach its community's sizable Hispanic population at public events, school bus safety classes, teen driver training classes, safety fairs, cultural festivals, local businesses, town hall meetings, and municipal advisory council meetings.

"The nice thing about the regional approach is the task forces we assemble, which typically stay together and continue to meet [about traffic safety] after the grant term is over," Taylor says. "It gets all the important players in a community together and gets them thinking about what they can do to fix the speeding problem in their community."

Enforcement

Enforcement was a cornerstone of the CHP's grant-funded activities in 2016. In addition to devoting more than 2,249,598 hours of regular patrol hours, during which officers issued 719,471 citations to speeding drivers, the RADIATES IV grant allowed officers to dedicate nearly 15,485 grant-funded overtime hours to speed enforcement. During the aforementioned overtime, officers cited 9,333 drivers, 6,433 of which were for maximum speed violations and 517 for unsafe speed violations.

"Like all law enforcement agencies, we are short on people," notes Taylor, who says the CHP maximized the grants' effectiveness by deploying officers to locations at times that were determined to be statistically more vulnerable to speed-related collisions. "With overtime hours, the grant gave us the ability to augment our regular road people with officers specifically focused on stopping speeding drivers."

Additionally, officers gave 2,335 verbal warnings to speeding motorists. "Warnings are designed to let the officer interact with the violator and educate them," Taylor continues. "It opens up a dialogue where the officer can explain why their speeding is an issue, and through that, hopefully change their behavior."

Enforcement was also part of its Area-wide regional traffic safety grants, according to the CHP. The Ukiah and Central Los Angeles Area offices conducted 42 and 127 roving patrols, respectively, during which officers issued 363 and 859 unsafe speed citations.

Outcomes

The extra attention that the CHP gave to speeding through its grant-funded activities yielded positive results. According to the CHP, 2016 data is not yet available, but there were 249 speed-related fatal collisions and 25,853 speed-related injury collisions in FY 2015, a decrease from 267 and 27,556, respectively, in FY 2014.

"As we await certification of the 2015 collision data, we've reduced the number of [speed-related] crashes, which is a positive in and of itself," Taylor concludes. "More importantly, though, I think we've broadened the level of understanding for the motoring public about the dangers of speeding."

Lessons Learned

- **Large problems demand extra resource:** Traffic safety grants can help law enforcement agencies scale up in order to confront their communities' biggest challenges.
- **State and regional approaches can work in concert:** Broad statewide approaches have advantages; so do narrow regional approaches. Using them in concert allows agencies to exploit the best of both.
- **Every interaction is an opportunity:** Whether officers issue a citation or merely a warning, every interaction with a speeding motorist is a chance to educate them about the consequences of speeding. A citation can impact their wallet; education can impact their behavior.

Traffic Safety through High Visibility Enforcement



By: **Commander Chris Olson,** *Patrol Bureau Commander,* Oro Valley, Arizona Police Department.

Police departments across the country are continually looking for innovative ways to improve traffic safety within their communities in an effort to reduce crashes. In 2013, the Oro Valley Police Department (OVPD) created a "High Visibility Enforcement" program known as "HiVE", in an attempt to raise traffic safety awareness and reduce crashes in two of the Town's most dangerous and closely located intersections. The "HiVE" concept included several key factors:

- Bring as much attention to the problem as possible,
- Be transparent by publishing all of the dates and times of the deployments in advance through traditional and social media sites.
- Be highly visible to the motoring public, and
- Demonstrate that the intent of the program is to raise awareness through education and not through ticket writing.

In order to bring attention to the traffic safety issues within the intersections, OVPD partnered with local television, radio, and print media. OVPD shared crash data demonstrating the need to reduce crashes within the intersections and committed to release all "HiVE" enforcement activity after each "HiVE" deployment. Moreover, OVPD asked the media sources to assist the department in providing the dates and times of each "HiVE" deployment in advanced to forewarn the public about the increased police activity. OVPD found the media outlets to be extremely receptive, reporting on the program numerous times throughout the year. Early morning TV news stations, as well as, radio stations constantly broadcasted "HiVE" dates and times. Some journalists even ensured that their social media sites regularly posted "HiVE" deployment and activity information.

Marketing and branding was considered key to increasing awareness. The OVPD Traffic Unit was tasked with designing a logo that could be used on publications, social media sites, television, and as decals for both the officer's motorcycles and motorcycle helmets. Once a design was drafted, OVPD hired a graphic's company put the professional touches on the design. Today, the "HiVE" logo continues to be significantly and readily associated with

our traffic safety program. The program's motto is "Be Aware, Be Safe."

Source: Oro Valley Police Department

Five times each month, OVPD placed 5-6 motorcycle officers within and around the intersections during morning or afternoon peak travel hours, essentially saturating the area with highly visible police officers to gain the attention of the traveling motorists. Officers were instructed to make all traffic stops in locations that were visible to other motorist's without compromising their safety. Upon each traffic stop, officers let the motorist know the reason for the stop first, and that the officer was participating in a "HiVE" deployment in an effort to educate drivers about the importance of traffic safety. At the end of each traffic stop, the motorist was provided with a "HiVE" pamphlet illustrating the program goals. On occasion, the officer would also provide the driver and any young children with a "HiVE" keychain and decal.

The most crucial element of the program involved protecting the trust between the police and the public. It was critical to demonstrate to the public that the program was not designed to be a "ticket writing" campaign. OVPD's goal was to increase awareness and education. To accomplish this, OVPD asked motorcycle officers to keep moving violation enforcement activity at around 30 percent. In other words, approximately 3 out of every 10 drivers would receive a citation for the moving violation they committed. By publishing the enforcement activity after each "HiVE" deployment, the public was able to see the department's focus remained on education and not enforcement.



Source: National Sheriffs Association

The OVPD "HiVE" program was deployed in two of the Town's most dangerous intersections for three years (2013, 2014, and 2015). A comprehensive analysis showed a significant reduction in crashes when compared to the three years before the "HiVE" program:

Intersection Crashes	Pre-HiVE (2010-2012)	HiVE (2013-2015)	Collision Reduction
Oracle at Suffolk	124	72	41.9%
Oracle at Magee	144	123	14.5%
Intersections Combined	*268*	*195*	*27.2%*

To help further understand the significance of the program's affect, especially at Oracle and Suffolk, OVPD partnered with a Ph.D. statistician during the analysis. Dr. Stephen Powers of Creative Research Associates concluded, "statistical testing would indicate that something other than chance contributed to the reduction of crashes at Oracle and Suffolk." In addition to the crash reductions, OVPD's analysis showed that police officers wrote citations for moving violations only 19.6 percent of the time. Demonstrating that our police department could improve traffic safety through education and limited enforcement.

Special note: In 2016, OVPD began to move HiVE deployments from intersection to intersection in an attempt to further promote the programs education and crash reduction success. Unfortunately, within a very short time, traffic crashes began to rise at the intersections of Oracle/Magee and Oracle/Suffolk, indicating no lasting residual effects from the previous three-year enforcement program. Moreover, OVPD did not see any tangible crash reductions at the other intersections. Police chiefs need to be aware that OVPD's HiVE success was directly related to a long-term focus on one or two specific intersections. Moving the HiVE from intersection to intersection seemed to dilute the high-visibility approach as motorist were no longer concerned about seeing heightened traffic enforcement activity at a specific intersection and resorted to previous poor driving behaviors.

If you would like to learn more about the OVPD "HiVE" program please contact, Commander Chris Olson at 520-229-4902 or at colson@orovalleyaz.gov.

About the author: Commander Olson is the Patrol Bureau commander for the Oro Valley Police Department. He has a M.Ed. in Human Relations from Northern Arizona University and is a graduate of the 244th Session of the FBI National Academy.

The Importance of Occupant Protection

According to NHTSA, in 2015 in the United States, seatbelt use in passenger vehicles saved an estimated 13,941 lives. Over the last two decades, great strides have been made to increase belt usage through bolstered laws, targeted education, and selective enforcement programs. As a result, the seatbelt usage rate in the U.S. has now risen to 89.7 percent; however, nearly 27.5 million people still don't buckle up. Data from NHTSA show that nearly half of the 22,441 occupants killed in crashes during 2016 were unbuckled. Additionally, more than 50 percent of passenger vehicle occupants killed at night were not wearing their seatbelts, compared to 40 percent killed during the daytime. In fatality collisions, men continue to outnumber women in not wearing seatbelts. Pickup truck occupants tend to be the lowest among any vehicle type in wearing. [1]

A Look at Seatbelt Laws

Every state has some form of seatbelt law on the books, however, the laws vary greatly from state to state. Most variability between states is regarding applicability of the law to occupants based upon age of the rider and which seat they are occupying. Seatbelt laws are also divided into two enforcement categories: primary and secondary. Primary seatbelt laws allow law enforcement officers to stop and ticket a driver or passenger for not wearing a seatbelt, without any other traffic offense taking place. In secondary seatbelt law states, the officer may issue a ticket for not wearing a seatbelt only when there is another citable traffic infraction.

According to the Governor's Highway Safety Association, as of 2019:

- 34 states have primary seatbelt laws for adult front seat occupants.
- 15 states have secondary laws for adult front seat occupants.
- 1 state has no primary or secondary seatbelt law for adults.
- 18 states include rear seats as primary enforcement.
- 10 states include rear seats as secondary enforcement.
- 21 states do not have seatbelt laws applicable to adult rear seat occupants. [2]

New Hampshire is the only state that has not enacted a primary nor a secondary seatbelt law for adults, although the state does have a primary child passenger safety law that covers all drivers and passengers under 18. [3] According to NHTSA seatbelt usage statistics from 2017, jurisdictions with stronger seatbelt enforcement laws continue to exhibit generally higher use rates than those states and territories with weaker laws. [4] If your state does not have a primary seatbelt law, it is highly recommended that you contact to your state special interest groups, legislators, and chief/sheriff's associations to express support in proposing stricter occupant protection legislation.

Occupant Protection Model Program Overview

Traffic safety is one of many priorities for any law enforcement agency. Traffic safety is a critical component of protecting communities and ensuring a high quality of life for residents. While each jurisdiction may have unique traffic concerns, occupant protection is widely accepted as one of the key areas for law enforcement to focus education and enforcement efforts in order to enhance traffic safety. Below is a basic overview of how agencies should approach occupant protection in their jurisdictions.

Policies

Each department should make enforcement of occupant protection laws a priority that is clearly stated in their policies, procedures, or general orders. The officers should be clear that this is a violation that will be strictly enforced to the extent allowed by law, and that this violation is a leading contributor to highway fatalities. Some law enforcement cultures still consider this law as a victimless offense, and the agency administrators should take steps to help change that attitude by clearly identifying this as a priority of the agency.

Agency policy should also require all officers, ride-alongs, and transported prisoners to wear seatbelts while in departmental vehicles. Exceptions to this should be very narrow in scope, or nonexistent. Managers should reinforce that the majority of line-of-duty officer deaths each year are typically traffic related. Further, the FBI's annual report of fatalities indicates that the majority of officers killed in traffic crashes are not wearing seatbelts. [5] Officer buy-in can also be improved by providing training such as Below 100, which emphasizes several key areas of officer safety.

Officer safety is only one reason for law enforcement managers to establish and enforce such policies. Officers who are not wearing their belts are less inclined to take enforcement action for occupant protection violations, and they also will not be modeling the correct behavior to the citizens of their community. These policies should be reviewed with officers annually.

Training

While most adult seatbelt statutes are relatively straightforward, the details of child passenger laws can be quite complex. Furthermore, the retrospective determination of seatbelt use by occupants involved in a collision is notably more technical than most officers realize. It is recommended that on an annual basis the officers receive some form of training covering the occupant protection laws of their state. Officers assigned to work traffic crashes should also receive training on identifying belt use during examination of the vehicles. Roll call is an excellent time to train on such topics, but document management systems, such as PowerDMS, allow uniform presentation of training materials and a subsequent test to ensure that the material is understood.

Child Passenger Safety Technician training is also highly recommended. This certification is usually a three to five-day course and requires ongoing education to maintain a certification. This training is not only beneficial for enforcement but is also very useful for public relations events. Safe Kids Worldwide is an example of an organization that offers a National Child Passenger Safety Certification. Agencies should strive to always have a Child Passenger Safety Technician available to the public during daytime hours. Personnel resources for this effort can be multiplied by partnering with the local fire/EMS agency, as many of them will offer members of their staff for certification as well.



Source: California Highway Patrol

Public Information and Education

The key to public education effectiveness is finding the best avenue for your department to reach the largest number people in your at-risk population. Social media has become a key tool for many departments in reaching their community members with their educational messages. It is highly recommended that each agency develop a strong presence on social media sites such as Facebook, Twitter, and Instagram. One key to increasing "likes" or shares" is to post often, vary what kinds of topics are being posted, and to always include a photo or video with each post. There are several resources available online that provide quality content that can be shared regarding occupant protection. An example of one of these sites is www.trafficsafetymarketing.gov, which provides free tool kits for many traffic safety topics and each national enforcement campaign. Use of these free, professionally produced materials provides agencies with limited resources, an opportunity to present highly effective and appealing messaging materials through whatever media outlets they choose.

Occupant protection public education should also be incorporated in other public information outlets the department has access to, such as public speaking events, city/department email updates to residents, news releases, and the department's website. Variable Message Trailers are also a good tool to target roadside education in problem areas. Occupant protection messages should correspond with national campaign movements such as Click or Ticket, but not be limited to these times of year. Many states and areas have access to additional tools, such as rollover simulators, and these are great tools to use during events such as high school football games, National Night Out, fairs, or other jurisdiction specific events.

As previously mentioned, each agency should strive to have certified Child Passenger Safety Technicians. The availability of these should be advertised to the community with instructions on how to set up appointments or when residents can get their seats checked. In addition, it is recommended that agencies facilitate car seat check events in their community on a regular basis. Agencies should consider partnering with local special interest groups to help raise awareness and attendance of these events. Safe Kids is an example of one of these agencies that has numerous chapters across the U.S. and can usually supply materials and additional technicians for events. For best results, events should be advertised, be on good weather days, and be done in locations that receive a high volume of citizens from your target audience. Day care centers, preschools, elementary schools, and local parks are good locations to reach the target audience. Ensure the checkpoint is well signed so those driving by know what and where the event is. When doing an event at schools or daycares, it is preferred that the event be done when parents are picking their children up from these locations. It is also recommended that the agency conduct Child Seat Checkpoints during the National Child Passenger Safety Week.

Seatbelt usage surveys should be conducted routinely; preferably monthly, but quarterly if monthly is not practical. Locations should vary around the jurisdiction to get a broad survey of usage, but follow-up surveys should also be conducted at some point to check progress against previous data from the same location. This data will help the department gauge the effectiveness of their efforts and provide intelligence on where to direct more education and enforcement. Results should be published to the community. Many jurisdictions have found success installing seatbelt use percentage signs along the major thoroughfares of their cities. The signs typically show the prior month's usage results along with the jurisdiction's record rate. This type of public information can serve as a social norming tool, wherein citizens that are not complying with seatbelt laws can clearly see the abnormality of their decision - hopefully beginning a rehabilitation of the thought patterns that contribute to lack of belt use. Those complying can also be reaffirmed in their decision to continue taking the widely accepted safest course of action, and those who forgot to buckle up may be reminded.

Another program to consider is a "Saved by the Belt Award." In some states, there is an organization that will actually issue the award for the agency once they receive a nomination. It is highly recommended that each agency participates in this program or start their own program if no others are available in the state. The basic premise is that an officer submits a person(s) for this award if they are involved in a collision where the use of the seatbelt by the occupant(s) is deemed by the collision investigator to have saved the person(s) from serious injury or death. The award should be issued in a public setting, such as a city council meeting. The media should be encouraged to publish a story on the event. At a minimum, the agency should post a photo and story about the presentation on their social media events. This is an excellent opportunity to earn some free media coverage and further spread the idea that seatbelts save lives.

Enforcement

A robust occupant protection program requires placing a priority on enforcing occupant protection violations. While these violations should be enforced anywhere state law allows, it is beneficial to prioritize enforcement in areas with a demonstrated compliance problem whenever practical. As mentioned earlier, seatbelt surveys aid in determining where and when problem areas are located. It is recommended that surveys be conducted in locations that receive 500-1,000 vehicles per hour. Most surveys analyze driver belt use, but occasionally the department should survey passenger belt use as well. Another area that should be analyzed is seatbelt use during collisions. Most, if not all, state collision reports have a field denoting what form of restraint each vehicle occupant was utilizing at the time of the collision. Officers completing the reports should be encouraged to thoroughly investigate belt usage during collision investigations to improve the quality of data available from these reports. With current technology, most agencies should have access to electronic collision reporting software and the ability to conduct statistical analyses from the data contained in the reports. Unfortunately, many agencies fail to use collision data to its full potential and simply look at high-collision locations and times. Statistical reports and/or maps can often be generated to highlight the highest locations/ times for collisions with unbelted occupants. Enforcement should be directed towards areas where collision trends show that belt use needs improvement. If the times of highest risk are at night, as indicated by national statistics, officers should use night time seatbelt enforcement details to enhance compliance and send the message that officers are on watch for such violations 24 hours per day.

Enforcement efforts should be increased during the national *Click It Or Ticket* campaigns, as well as any similar state campaign. It may be helpful for the agency to offer some type of non-monetary incentive for officers who perform in an exemplary manner during these mobilizations through their enforcement and/or public education efforts. Some departments also offer incentives such as free lunch with the chief, or even time off for exceptional performance. Posting enforcement results by officers periodically, particularly during campaign periods, may inspire increased participation from officers that are not prioritizing efforts in this area as much as others. An end of the year award for occupant protection efforts is also highly recommended and does not have to be limited to just enforcement outputs as the measure of success. Many other factors, such as the number of car seats checked or implementation of innovative education efforts, can deserve recognition as well.

Enforcement details should be conducted on a regular basis for occupant restraint violations. These details should include a spotter and at least one vehicle assigned to pull or wave the violators over after the spotter calls them out. The spotter should be in a good position to observe violations, and this usually means out of their car near an intersection. Being out of the car also puts the officers in a much better position to observe child seat violations. Many agencies have found great success with putting an officer/spotter in plain clothes at an intersection or having them dress like a road crew worker while looking for violations. Since seatbelt compliance percentages are often lower at night, details should be conducted after dark in well-lit areas that provide the correct lighting to observe infractions. Night time details also frequently lead

to the discovery of other crimes, such as impaired driving or drug violations, which can be an additional incentive for officers to participate in these details and further increase the safety of the roadways in your jurisdiction.

Evaluation of Efforts

The overall effectiveness of a department's occupant protection program should be routinely (monthly or quarterly) evaluated to determine the effectiveness of efforts over the last evaluation period. Strategies (enforcement, education, incentives, etc.) should be updated following each evaluation. Each agency is also strongly encouraged to compete in state or national traffic safety challenges. While the highest scoring applications do receive recognition, and in some states actual financial or equipment incentives, the main benefit to such competitions is a chance to thoroughly review efforts from the last year, evaluate their effectiveness, and then compare strategies and outcomes against industry best standards and other agencies. Participants should not be discouraged if their agency does not place or win, but rather, review the winning agency applications and look for strategies and ideas to improve their own program.

Conclusion

Law enforcement managers can make a significant impact on traffic-related deaths and injuries in their jurisdiction by prioritizing enforcement and education efforts related to occupant protection laws. By integrating the recommendations above, law enforcement agencies can build an occupant protection program that is supported by officers, highly visible to the public, data-driven, and based upon widely accepted best practices.

Notes:

1. "Seatbelts," NHTSA. Accessed July 5, 2017, https://www.nhtsa.gov/risky-driving/seat-belts.
2. "Seatbelts," Governors Highway Safety Association. http://www.ghsa.org/state-laws/issues/Seat-Belts.
3. Ibid.
4. "Traffic Safety Facts, Seatbelt Use in 2017 – Overall Results," NHTSA. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812465.
5. "FBI Releases 2016 Preliminary Statistics for Law Enforcement Officers Killed in the line of Duty," FBI. Accessed July 5, 2017, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2016-preliminary-statistics-for-law-enforcement-officers-killed-in-the-line-of-duty.

CHAPTER 2: OFFICER SAFETY

Research in Brief: Officer-Involved Collisions: Magnitude, Risk Factors, and Prevention

By: **Hope Tiesman,** *Research Epidemiologist,* National Institute for Occupational Safety and Health; **Jeff Rojek,** *Associate Director,* Center for Law & Human Behavior, University of Texas at El Paso; **Geoffrey P. Alpert,** *Professor,* University of South Carolina; and **Scott Wolfe,** *Assistant Professor,* University of South Carolina

In 2016, law enforcement officer deaths rose to their highest level in five years, driven by firearm-related deaths. [1] However, the law enforcement community should not lose sight that motor vehicle events, including collisions and being struck by moving vehicles, have been a leading cause of death for many years. [2] In addition, there are even more collisions that do not result in fatalities, but can cause injuries and property damage. In California, for example, it is estimated that there are more than 100 non-fatal collisions for every fatal collision. [3] Vehicle collisions can have a tremendous emotional, physical, and financial impact on officers, their families, and their departments; yet, few formal research studies on these effects exist. Fortunately, several recent efforts have started to fill this knowledge gap.

In 2007, the California Commission on Peace Officer Standards and Training (CA POST) brought together law enforcement professionals and researchers to develop knowledge on officer-involved collisions, which led to the SAFE Driving campaign. [4] In 2011, the National Officer Safety and Wellness Working Group highlighted the need for better knowledge on collisions and effective reduction programs. [5] Subsequently, studies have been funded by the National Institute of Justice (NIJ), Bureau of Justice Assistance (BJA), and National Institute for Occupational Safety and Health (NIOSH) on this officer safety issue.

The Magnitude of Officer-Involved Collisions

One study, funded by the NIJ, examined over 35,000 officer-involved collisions in California from January 2000 to December 2009. [6] In that 10-year period, there were 39 officer fatalities, and 21 percent of the collisions (7,684) resulted in an injury to an officer. The collision data also revealed that seatbelt use was inversely associated with injury severity. Seatbelts were less likely to have been used in collisions resulting in severe injuries and death. Nearly 77 percent of the collisions (26,875) involved both a law enforcement vehicle and civilian vehicle. In these collisions, civilians were more likely to be killed than officers. Civilians represented 73 percent of the total fatalities, and officers represented 27 percent.

What Increases an Officer's Risk for a Collision?

A second study, funded by the BJA, examined collisions across eight California law enforcement agencies. The researchers examined collisions, training records, and driving policies, as well as conducted surveys and focus groups with officers. The primary predictor of an on-duty collision for officers was having a collision off duty. Family responsibilities such as having children and being in a committed relationship reduced the likelihood of an officer-involved collision. The survey also revealed 42 percent of officers reported wearing seatbelts "all of the time" on duty, and 34 percent reported wearing them only "some of the time" or "rarely." Factors associated with seatbelt use included feeling treated fairly by supervisors in organizational measures such as promotions and discipline, as well as having supervisors enforce departmental seatbelt policy. Officers with a risky driving attitude, as measured by a questionnaire, and those with prior on-duty collisions were less likely to report wearing seatbelts. [7]

Preventing Officer-Involved Collisions

During a six-month period in 2009, the Las Vegas (Nevada) Metropolitan Police Department (LVMPD) lost three officers in vehicle collisions. In response, the LVMPD developed a comprehensive collision prevention program that included a campaign to increase awareness of driving hazards, stringent driving policies, and an expansion of driver training. The campaign, titled 365 Alive, included visual cues such as decals in patrol cars and posters in hallways and parking garages. It also included daily driving safety messages distributed at roll calls. Policy changes included the introduction of or re-emphasis on seatbelts, intersection crossings, speed caps, and texting policies. Driver training was expanded to eight hours of in-service training annually for officers in their first three years of service and four hours of training every other year for officers with more than three years of service. NIOSH and NIJ funded a scientific evaluation of this program, which showed significant reductions in motor vehicle collision and injury rates after the program's implementation. There were also reductions in restricted and lost workdays, as well as in workers' compensation costs. [8]

Collectively, these studies have increased the knowledge of on-duty vehicle collisions. Moreover, the LVMPD has demonstrated that simple safety messaging and changes to training and policy can change culture. Prince George's

County (Maryland) Police Department (PGPD) is another example of an agency that uses incentives, education, and safety messages through its Arrive Alive campaign to develop and sustain a safe driving culture. [9] The next step for addressing officer-involved collisions is to identify initiatives like the LVMPD and PGPD efforts and determine how the programs work in agencies of different sizes and with different demands and resources.

Notes:

1. National Law Enforcement Officer Memorial Fund, "135 Law Enforcement Fatalities Nationwide in 2016," news release, December 29, 2016.
2. Byron Gustafson and Paul Cappitelli, "SAFE Driving—The Role of the Chief," *The Police Chief* 77, no. 3 (March 2010): 38–41.
3. Ibid.
4. Janna Munk and David Kinaan, "SAFE Driving Campaign: Building a Culture of Courage to Save Law Enforcement Lives," Officer Safety Corner, *The Police Chief* 83, no. 7 (July 2016): 12–13.
5. Darrel Stephens, Steven Edwards, and Mora Fiedler, *OSW Group Annual Summary: Issues and Recommendations Discussed for Improving the Wellbeing of Police Officer* (U.S. Department of Justice, Office of Community Oriented Policing, 2012); Darrel Stephens, Mora Fiedler, and Steven Edwards, *OSW Group Meeting Summary: Vehicle Operation, Risk Management, and Problem-Based Learning*, April 25, 2012 (U.S. Department of Justice, Office of Community Oriented Policing Services, 2013).
6. Scott E. Wolfe et al., Evidence-Based Solutions to Reduce Law Enforcement Officer Vehicle Crashes (forthcoming); Scott E. Wolfe et al., "Characteristics of Officer-Involved Vehicle Collisions in California," *Policing: An International Journal of Police Strategies and Management* 38, no. 3 (2015): 458–477.
7. Andrew Hansen, "The Influence of Department Policy and Accountability on Officer-Involved Collisions," *Policing: An International Journal of Police Strategies and Management* 38, no. 3 (2015): 578–594.
8. Hope Tiesman et al., "Evaluation of a Motor-vehicle Crash Prevention Program in Law Enforcement," Traffic and Vehicle Safety for Law Enforcement: Keeping Officers Safe on the Road (presentation, International Association of Chiefs of Police Conference, San Diego, CA, October 2016).
9. Kirk McLean, "Taking Care of Your Own: Sustaining a Culture of Crash Prevention Efforts in Law Enforcement," Officer Safety Corner, *The Police Chief* 84, no. 3 (March 2017): 12– 13.

Safety for Law Enforcement Officers – Still a Priority

By: **Hope M. Tiesman, PhD,** *Research Epidemiologist,* National Institute for Occupational Safety and Health, Morgantown, West Virginia; **Rebecca Heick, PhD,** *Assistant Professor of Public Health,* MCPHS University, Boston, Massachusetts

Between 2013 and 2014, the number of officers who died in the line of duty increased by 24 percent. In 2014, 50 officers were killed in firearm incidents, and 49 died due to motor vehicle events. [1] In the last decade, one officer a week, on average, has been killed on U.S. roads (2005–2014 = 61.9 deaths annually). [2]

Even though motor vehicle crashes are a leading cause of job-related deaths among law enforcement officers, data on motor vehicle injury and crash trends are scant. The National Institute for Occupational Safety and Health (NIOSH) embarked on a comprehensive statewide study of motor vehicle safety among law enforcement officers to better understand these issues. The study was conducted in one state (Iowa); however, the results and recommendations are useful to law enforcement leaders across the United States.

A State-Based Study

In 2011, 136 agencies were randomly selected for the study from a list of all Iowa law enforcement agencies, stratified by type (municipal, state patrol, sheriff) and size. Of those 136 agencies, 60 agencies (44 percent) participated, representing 1,466 officers. Surveys were distributed by agency leadership and returned to researchers using a self-addressed stamped envelope; individual officer response rate was 79 percent (1,157 responses). The survey included questions on occupational characteristics, motor vehicle training, safety practices and perceptions, and motor vehicle crashes (MVCs) and "struck-by" events in the last three years.

Key Findings

Most officers believed driver training was critical to their safety (96 percent); however, only half of the respondents believed that academy-provided driver training adequately prepared young officers to safely function in the field, and only 12 percent believed the average academy recruit had driving skills sufficient to safely operate a law enforcement vehicle. Additionally, only 29 percent of the officers received annual motor vehicle training. Hands-on training, such as pursuit driving, was reported about one-third of the time. While most officers reported having a motor vehicle policy, such as general operations or standard operating procedures, only 66 percent had received any training on the actual policy. The least common elements of written motor vehicle policies were speed restriction when using lights or sirens (27 percent of policies) and cellphone use restrictions (39 percent).

MVCs and struck-by events were reported as common. In the prior three years, 20 percent of the officers had at least one MVC, and 16 percent reported being struck by or nearly struck by a passing motorist. Most of the reported MVCs occurred during daylight (49 percent), in clear weather (70 percent), during non-emergency responses (64 percent), and at speeds lower than 50 mph (79 percent). Additionally, nonfatal roadside incidents mostly occurred during daylight (60 percent) and in clear weather conditions (60 percent). Nearly half of the non-fatal roadside incidents occurred during traffic stops (47 percent).

Finally, 81 percent of officers reported wearing a seatbelt "all of the time," but only 8 percent of officers reported wearing reflective gear while outside their patrol cars on highways.

Recommendations

Motor Vehicle Training

Agencies could consider providing more opportunities for motor vehicle training and provide officers with more hands-on experience. A study by the California Commission on Peace Officer Standards and Training (Cal POST) found that behind-the-wheel training resulted in the fewest collisions when conducted every two years. [3] Also, since many officers felt that academy-provided driver training was insufficient, states and agencies could conduct analyses of their current training programs to assess the consistency and effectiveness of their motor vehicle training efforts. Expanding hours of motor vehicle training and providing more hands-on training may be warranted.

Use of Personal Protective Equipment

In this study, reported seatbelt usage was high. Agencies should strive for 100 percent seatbelt use by implementing strong policies and supporting officers in the wearing of seatbelts. Recently, the United States' largest police unions and a coalition of major city police chiefs called all agencies to implement mandatory seatbelt use. [4] The use of reflective gear was very low; wearing high-visibility vests can significantly reduce an officer's chances of being struck on the roadway. [5] Agencies should encourage officers to wear high-visibility apparel whenever they work in the vicinity of moving vehicles.

Motor Vehicle Policy

An uncommon component of motor vehicle policies was cellphone restrictions. Research among commercial drivers shows that cellphone use is associated with an increased crash risk. [6] Agencies should consider implementing policies that reduce distractions in patrol cars by restricting the use of cellphones while officers are driving.

Another uncommon component was speed restriction. Both the National Highway Traffic Safety Administration and Cal POST found that "driving too fast for conditions or in excess of posted speed" was a leading factor in many officer-involved crashes. [7] Agencies could implement and enforce policies that restrict excessive speed.

Motor Vehicle Safety Culture

Experienced officers were less likely to have had an MVC and more likely to use safe driving techniques than those with less law enforcement experience. Mentoring programs may help to change driving culture, and formal mentoring programs in law enforcement have led to higher job satisfaction and a stronger work ethic in those mentored. [8] Agencies should also consider adding personal testimonies of officers who have been involved in MVCs into their motor vehicle training like those used in such programs as Below 100, since personal stories have been shown to have a large impact. [9]

Motor vehicle–related events have prompted some agencies to make significant changes to their motor vehicle policies and training in an attempt to change their driving culture. One such agency is the Las Vegas Municipal Police Department, whose crash prevention program's impact on MVCs and related injuries and costs is currently being evaluated through a jointly funded effort by the National Institute of Justice and NIOSH.

Action Items

- Encourage or require seatbelt use.
- Provide periodic motor vehicle training.
- Include personal testimonies of officers who have been involved in MVCs into motor vehicle training.
- Add cellphone restrictions and speed restrictions into current written motor vehicle policies.
- Encourage or require officers to use reflective gear while working in the vicinity of moving vehicles.

Notes:

1. National Law Enforcement Officers Memorial Fund (NLEOMF), *Preliminary 2014 Law Enforcement Officer Fatalities Report*, http://www.nleomf.org/assets/pdfs/reports/Preliminary-2014-Officer-Fatalities-Report.pdf (accessed January 5, 2015).
2. NLEOMF, "Causes of Law Enforcement Deaths," http://www.nleomf.org/facts/officer-fatalities-data/causes.html (accessed January 5, 2015).
3. California Commission of Peace Officer Standards and Training (CalPOST), *POST Driver Training Study* (Sacramento, CA: CalPOST, 2009).
4. Kevin Johnson, "Police Union, Chiefs Call for Mandatory Armor, Seatbelts," *USA Today*, November 20, 2014, http://www.usatoday.com/story/news/nation/2014/11/20/mandatory-armor-seat-belts/19326349 (accessed March 4, 2015).
5. Federal Motor Carrier Safety Administration (FMCSA), *Synthesis of Literature Relating to Cellular Telephone/Personal Digital Assistant Use in Commercial Truck and Bus Operations* (April 2011), http://ntl.bts.gov/lib/51000/51200/51275/Cell-PDA-Use-in-Commercial-Truck-and-Bus-Operations.pdf (accessed March 4, 2015).
6. Ibid.
7. National Highway Traffic Safety Administration (NHTSA), *Characteristics of Law Enforcement Officers' Fatalities in Motor Vehicle Crashes* (January 2011), http://www-nrd.nhtsa.dot.gov/Pubs/811411.pdf (accessed March 4, 2015); CalPOST, *POST Driver Training Study.*
8. Harvey Sprafka and April H. Kranda, *Best Practices Guide: Institutionalizing Mentoring into Police Departments* (Alexandria, VA: International Association of Chiefs of Police), http://www.theiacp.org/Portals/0/pdfs/Publications/BP-Mentoring.pdf (accessed March 4, 2015.)
9. Mitch Ricketts et al., "Using Stories to Battle Unintentional Injuries: Narratives in Safety and Health Communication," *Social Science & Medicine* 70 (2010): 1441–1449.

Below 100 Initiative: A Reality Check on Officer Safety



By: **Dale Stockton,** *Founder,* Below 100

There's a different conversation that's taking place around the country regarding officer safety, and it is being driven by Below 100, a commonsense training program that focuses on areas under an officer's control. Consider those last few words for a moment: *areas under an officer's control.* It is this perspective that has made Below 100's approach so different from others. Until recently, most discussions about officer safety centered on suspect actions and tactics designed to thwart the attack of an assailant. It is not that these are without merit. They're actually very important and should continue to be part of officer safety training. However, we have been so focused on the bad guy that we have often ignored the elephant in the room: culpability on the part of the officers who have lost their lives. Admittedly, this makes some uncomfortable. After all, officers who die in the line of duty have made the ultimate sacrifice. Reflect on this: what would those fallen officers want to share about how they died? Would they want their mistakes repeated, resulting in further loss? We all know the answer, and it's important that we make sure those who have died are never forgotten, including the lessons that can be learned. "Honor the fallen by training the living," has become a mantra for Below 100 trainers, and it should be the guiding principle for every trainer who stands in front of a group of officers, regardless of the subject.

When the concept of Below 100 was first coming together, the evidence and magnitude of preventable losses were so compelling that I assumed there must be an existing effort underway to address issues like seatbelt use, wearing body armor, speed, situational awareness, and complacency. Although there were initiatives or training courses that addressed parts of the problem, there really wasn't an overarching, comprehensive approach to tackle the thorny issue of addressing officer responsibility. In other words, no one had effectively said, "Look what we are doing to ourselves. We have to change this." The human tendency to blame others (the bad guys) for our losses rather than look at our own shortcomings had caused a degree of deadly ignorance.

Don't hear the wrong thing. I know full well that bad guys kill good cops. I also know, after reading more than 5,000 line-of-duty death summaries going back to 1980 that we, as a profession, have long failed to address areas that are squarely under our control, areas that have little to do with an armed assailant. In terms of making a difference, which of these do you have more control over?

- A determined assailant who is willing to set up an ambush and die trying to kill an officer;
- Actions and decisions that you make in regard to use of safety equipment, the way you drive and how you handle a call?

The need to place increased emphasis on areas under an officer's control becomes readily apparent with a simple examination of how a large portion of our losses are occurring. Over the last twenty years, losses due to vehicle-related incidents have accounted for approximately 25 percent *more* deaths than gunfire. Data from an extensive NHTSA review shows that half of fatal police crashes are *single-vehicle crashes.* The primary collision factor is overwhelmingly speed too fast for conditions. Just as troubling is the fact that approximately half of all police officers choose to operate their vehicles while not wearing their seatbelts. This has cost hundreds of lives and destroyed thousands of careers due to incapacitating and career-ending injuries. When it comes to speed, single-vehicle crashes and failing to wear a seatbelt, it is very, very difficult to lay the blame at the feet of the bad guy. As the saying goes, "This one is on us." And it's definitely up to us to change it.

A Quick Review

Below 100 is comprised of five very straightforward tenets:

1. **Wear your seatbelt.**
2. **Wear your vest.**
3. **Watch your speed.**
4. **WIN: What's Important Now?**
5. **Remember: Complacency Kills!**

Pretty simple, right? Yes, but they're definitely not easy. Simple to understand does not equate to being easy to make happen. Law enforcement culture has a long and storied history of resisting change, and tragically, many officers have died as a direct result of falling into a pattern of behavior that was facilitated by department culture.

How to Make a Difference: Vehicle Operations, Ambush Attacks, and Officer Health

Vehicle operations and roadway practices are areas where we can definitely improve, and it's time for everyone who wears a badge to take substantive steps to increase officer safety through improved vehicle safety. Seatbelts should be a given; speed awareness is critical, and officers need to wear reflective gear when investigating roadway incidents or directing traffic. We lose far too many officers to single-vehicle crashes where speed is the primary collision factor, and many officers are struck and seriously injured because

they are not seen while standing on or near the roadway. These events do not make the headlines like an ambush slaying, but they are just as deadly, far more prevalent, and an area that we can absolutely change.

There is little doubt that the level of hostility to law enforcement remains high, and it's definitely a time for vigilance. Body armor should always be worn when you're in a recognizable law enforcement role. This includes training days and administrative or office assignments. If you're in a plainclothes assignment, consider your armor as a highly-recommended option and a mandate when working the field or making suspect contacts. A suit coat or polo shirt offers zero ballistic protection. Body armor has already saved many thousands of lives, but it only works when you wear it.

Improved tactics are paying off, but complacency can turn any situation deadly in an instant. The ability to self- or buddy-treat gunfire wounds is making a huge difference in saving lives. Every officer should carry a tourniquet (on his/her person) and know how to use it. Check premise history when available, especially on domestic violence calls. When situationally appropriate, consider having the reporting party come to the curb for a meet instead of going to the door. Officers should consider using a passenger-side approach during traffic stops and continually use contact and cover techniques when working with another officer. If you're not familiar with contact and cover, check Google. You'll find it is super simple, and it works.

After vehicles and gunfire, heart attacks have consistently been the third leading cause of death for police officers. During the period of 2014 through 2016, 43 officers succumbed to duty-related heart attacks. This is not an "old guy" problem. The youngest was only 23, another was only 26 and many of the officers were in their 30's and 40's. It's time to acknowledge this deadly killer and to become proactive. No one has more control over their health than the individual officer. At a minimum, officers should know their blood pressure, cholesterol level, body mass index, and family history—then do something about it!

Courageous Conversations

Below 100 takes the position that it is the responsibility of every person wearing a badge, regardless of rank or assignment, to take individual and collective responsibility for officer safety. This includes having the courage to talk to another officer about the five tenets outlined above. Going into dangerous situations without adequate cover or engaging too quickly has been the story behind many police losses. If you know an officer who tends to push the envelope or take unnecessary chances, have the courage to talk to them. Tell them that you care and that their family and department need them. Point out that they're actually endangering others who may have to come to their rescue. Confronting a fellow officer is never easy, but it's far better than going to their funeral. Don't wait because you may not get a second chance. Every leader and trainer should remember that ignored behavior is condoned behavior.

Honor the Fallen

None of the officers whose names are on the National Law Enforcement Memorial thought their final tour of duty would take their life. For many, their deaths could easily have been prevented. It is clear that we can dramatically improve officer safety by simply exercising common sense. That's the operational principle of Below 100. Every line-of-duty loss should be reviewed by trainers, especially FTOs, and information gleaned should be shared with others and at briefing. We must honor the fallen by training the living. They would want nothing less from us. Remember, the life you save may be your own. For more information on Below 100, check www.Below100.org.

Destination Zero Program

The Destination Zero Program is coordinated by the National Law Enforcement Officers Memorial Fund in cooperation with the U.S. Department of Justice, Bureau of Justice Assistance, and the VALOR Initiative. Destination Zero has a goal of helping law enforcement agencies improve the health and safety of law enforcement officers. The program also fosters a platform that provides all law enforcement agencies with the ability to research successful and/or promising officer safety and wellness programs and to identify the resources necessary to begin their own risk management initiatives. [1]

Each year, the program recognizes officer safety and officer wellness programs that proactively engage employees in initiatives that increase overall officer wellness or reduce line-of-duty injuries or deaths. Awards are presented in four categories: general officer safety, officer traffic safety, officer wellness, and comprehensive safety. The award winners are selected and acknowledged during Police Week ceremonies in Washington, D.C. [2]

The Snohomish County, Washington, Sheriff's Office (SCSO) was selected in 2017 as the winner in the Officer Traffic Safety category. At the end of 2015, after sustaining 11 on-duty collisions that resulted in major injury to either an employee or a county resident, the Snohomish County Sheriff's Office (SCSO) introduced a new mindset to their officers: "Get there safe and get there alive." This was a change from the older philosophy of "Get there first get there fast."

The SCSO began working to incorporate the Below-100 training and its tenets into in-service training and into departmental messaging. All the agency supervisors attended a presentation by Kim Schlau, the mother of two teenage girls killed in a collision with an Illinois state trooper speeding to a call. The presentation was recorded and has been included in mandatory roll call training. The Snohomish County Sheriff's Office has distributed Below-100 posters to all their precincts, offices, and contract city locations.

SCSO updated their pursuit policy to be more restrictive and created a Driving Review Board (DRB), which meets monthly to review all agency pursuits and on-duty collisions. The Sheriff's Office is also installing telematics into all patrol cars. This new technology will allow the department to identify unsafe driving behaviors that can be addressed by supervisors and in training. [3]

Police departments can quickly learn about best practices and model programs by visiting the Destination Zero website at: http://www.nleomf.org/programs/destination-zero/. At this site, one can find hundreds of resources ranging from policies and procedures, officer wellness programs, traffic safety information, equipment, and presentations that will be helpful to law enforcement leaders.

Notes:

1. National Law Enforcement Officers Memorial Fund, "About Us," http://www.nleomf.org/programs/destination-zero/dz-about.html (accessed May 21, 2017)
2. Ibid.
3. National Law Enforcement Officers Memorial Fund, "Destination Zero," http://www.nleomf.org/programs/destination-zero/dz-about.html (accessed May 21, 2017)

Police Pursuits: Trends and Emerging Technology

The National Highway Traffic Safety Administration (NHTSA) defines police pursuits, pursuit terminations, and pursuit fatalities as follows:

A police pursuit is defined as an event initiated by a law enforcement officer operating an authorized motor vehicle giving notice to stop (either through the use of visual or audible emergency signals or a combination of emergency devices) to a motorist who the officer is attempting to apprehend, and that motorist fails to comply with the signal by either maintaining his/her speed or taking evasive action to elude the officer's attempt to stop the motorist. A pursuit is terminated when the motorist stops, the attempt to apprehend is discontinued by the officer, or at the direction of a competent authority. A police pursuit related death is defined as all fatalities recorded in a pursuit-related crash. [1]

In *Motor Vehicle Crash Deaths Related to Police Pursuits in the United States*, Dr. Fred Rivera found that "approximately 300 lives are lost each year in the United States from police pursuit related crashes, and one third of these are among innocent people, not being pursued by the police." Using the NHTSA Fatality Analysis Reporting System, "there were 260-365 police pursuits ending in a fatality annually in the U.S. for a total of 2654 crashes involving 3965 vehicles and 3146 fatalities during a nine year study period." [2]

Law enforcement leaders, researchers, and the general public have been working on training, policies and procedures, and emerging technologies in an effort to mitigate high-risk and unnecessary police pursuits. The Highway Safety Committee of the IACP has proactively initiated steps to adopt innovative pursuit training and model polices. For more information see: "P.U.R.S.U.E.: The Training Video" article in the *Police Chief* magazine which provides additional details for law enforcement leaders on this topic to include information about the P.U.R.S.U.E. training DVD.

Emerging technologies offer some potential alternatives to police pursuit, however, need further study. Some of the technologies being considered to mitigate the risk of pursuits include spike strips, OnStar Stolen Vehicle (SVS), aerial vehicles, nets and barricades, and StarChase. Of course, these technologies must be considered with many other factors including the type and size of the police department, fiscal resources, and training. [3]

The StarChase technology is particularly interesting and has been deployed by several law enforcement agencies in the United States. StarChase consists of a compressed air-launcher system mounted behind the grille of a police vehicle. The launcher has a laser target which discharges an adhesive projectile/tag containing a global positioning system (GPS) module that will transmit GPS coordinates to law enforcement via a digital roadmap. [4]



StarChase System.
Source: *Pursuit Technology Impact Assessment, Version 1.1* report

This tagging and tracking technology has been studied by the Johns Hopkins Applied Physics Laboratory supported by a grant awarded by the National Institute of Justice. According to the *Pursuit Technology Impact Assessment, Version 1.1* report, published in January 2017, the "end

users' opinion of StarChase is that it is a helpful pursuit management tool, but that it is not a comprehensive solution for avoiding or successfully resolving all possible pursuit scenarios." Potential complicating factors include Fourth Amendment considerations of deploying a GPS device on vehicle. Police departments will need to consult the latest court decisions in the consideration of using any GPS tracking system. [5]

Notes:

1. Definitions of Pursuits (In House Definitions) 2004. National Highway Traffic Safety Administration, US Department of Transportation, Washington, DC, Fatality Analysis Reporting System.
2. Rivara, Fred and C.D. Mack, "Motor Vehicle Crash Deaths Related to Police Pursuits in the United States," *Injury Prevention* (2004); 10; 93-95
3. Gaither, Morgan et al, "*Pursuit Technology Impact Assessment, Version 1.1*" (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/250549.pdf, (accessed May 31, 2017).
4. Ibid.
5. Ibid.

The Dangers of Vehicle Pursuits: New Emerging Issues

By: **Richard Johnson, PhD,** University of Toledo, Ohio and **Harry Dolan,** *Chief (ret.),* Raleigh, North Carolina, Police Department

Adapted with permission. The International Association of Chiefs of Police, (2016). Copyright held by the International Association of Chiefs of Police, 44 Canal Center Plaza, Suite 200, Alexandria, Virginia 22314 USA.

As long as crime has existed, criminals have been attempting to elude justice. The invention of the automobile gave criminals one more way to attempt to escape the grasp of law enforcement. While the use of motor vehicles by criminals is widespread, one could assume that vehicle pursuits have become safer for officers over time. Improvements in vehicle safety technology have made cars more maneuverable and safer, increasing the likelihood of surviving a high-speed crash. Advances in emergency trauma medicine have also increased the survival rate of traffic crash victims. Today, most law enforcement agencies have policies limiting the circumstances under which a vehicle pursuit may occur, how it will be monitored by management, and when it will be called off to avoid undue risks to the officers and the public. Police pursuit training has become more extensive and realistic, involving intense computer simulations and hands-on practice with real vehicles. Finally, anti-pursuit technologies have become common, such as devices used to deflate the tires of suspects' vehicles.

But have pursuits really become safer? Both authors have encountered high-speed vehicle pursuits that ended in the fleeing suspect surrendering to the police, without injury to officers, citizens, or suspects. On the surface, these incidents appear to be textbook successes. Many of these same pursuits, however, have also involved numerous assisting officers racing across the city at extremely high speeds, traveling through stop signs and red lights at rush hour, to assist in the pursuit by trying to get ahead of it to lay tire-deflation devices in the path of the pursuit. The authors have witnessed officers, miles from the pursuit, racing through intersections at breakneck speeds, just narrowly missing the cars of innocent people on their way home from work or school—even witnessed assisting officers, pumped with adrenaline, loudly cursing innocent citizens who did not move aside fast enough. While officers in direct pursuit are often governed by strict department policies limiting the pursuit to reasonable speeds, additional officers who are not in direct pursuit are often traveling at unsafe speeds all across the area to assist in the pursuit.

These observations led to a broader examination of the risks vehicle pursuits pose to officers. This broader study examined not only officers in direct pursuit, but also the danger and risks to officers assisting in these pursuits. This analysis of officer deaths associated with vehicle pursuits revealed that police vehicle pursuits have not become safer over time. In fact, some types of officer deaths associated with pursuits have been on the increase for the last few decades. The study reveals trends in officer deaths related to pursuits and provides a backdrop for an exploration of suggestions to mitigate the trends and understand the potential effects on police pursuit policies and practices.

Study Methodology

The study began with an investigation of law enforcement officers killed while involved in vehicle pursuits from 1960 through 2011. Data were gathered on all police officers killed in a motor vehicle–related death from the Law Enforcement Officers Killed and Assaulted (LEOKA) reports published annually by the Federal Bureau of Investigation (FBI), death descriptions offered on the Officer Down Memorial Page website, and archived newspaper articles surrounding each officer's death. These information sources were reviewed to identify officers whose deaths were associated with a vehicle pursuit in some way. This review identified 455 officer deaths related to vehicle pursuits during the 52-year study period.

Data were gathered on the role each of these officers played in the pursuits, revealing that 75 percent were directly involved in pursuing a fleeing suspect vehicle at the time of their deaths. Another 19 percent were involved in some sort of blocking activity (such as creating a roadblock or deploying tire deflation devices), and the remaining 6 percent were traveling to catch up to the pursuit or get ahead of it to establish a blocking position.

It was originally anticipated that the data would reveal a gradual decline in officer pursuit-related deaths for several reasons. First, advances in trauma medicine and EMS services at the scene of accidents have significantly reduced citizen deaths in automobile accidents over the last four decades. Second, improvements in automobile engineering have made vehicles significantly safer. Third, officer pursuit training has increased in quantity and quality, now including video-based simulations, as well as actual vehicle operations on a closed track. Fourth, most law enforcement agencies have developed detailed written policies governing when and how vehicle pursuits will be conducted, with some agencies limiting pursuits to cases of violent felony offenses. A few agencies have even banned pursuits entirely. Finally, the last four decades have witnessed the development and proliferation of tire-deflation devices used by police departments. These facts, taken together, would lead one to anticipate that, over time, the number of police pursuits has decreased, and when pursuits occur, they would be less likely to result in the death of an officer. The results of the analysis, however, only partially meet these expectations.

Study Results

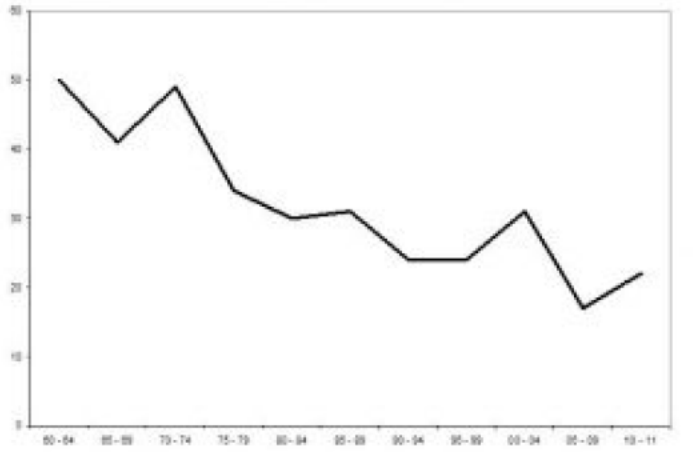


Figure 1. Officers killed while persuing a fleeing vehicle 1960-2011

Figure 1 is a line graph of law enforcement officers who were directly involved in a pursuit by chasing the fleeing suspect vehicle at the time of their deaths. These officers died by losing control of their vehicles, colliding with the suspects' vehicles, colliding with another police vehicle, or colliding with an innocent third party. This figure demonstrates that, as anticipated, this role in pursuits decreased in lethality over time. The number of officers who died while involved in direct pursuit gradually declined over the last five decades, from 50 officers killed between 1960 and 1964, to 17 killed between 2005 and 2010. It appears that the advances in pursuit policies, medical resources, and vehicle technology have paid off in officers' lives saved during direct pursuits.

Blocking Activities Deaths

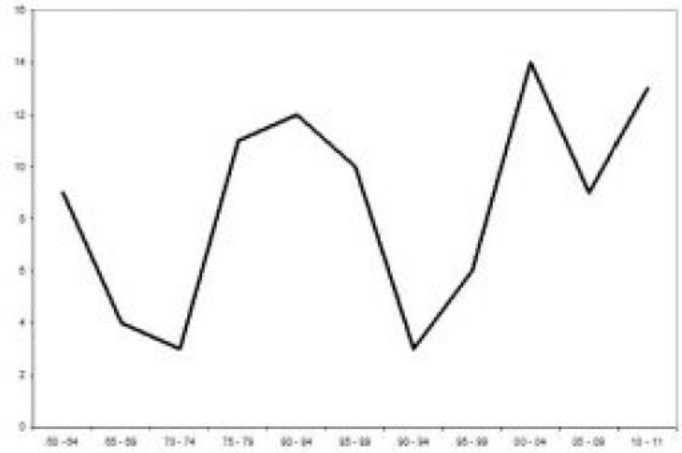


Figure 2. Officers killed while engaged in blocking activities 1960-2011

Approximately 19 percent of the pursuit-related officer deaths occurred to officers attempting to establish some sort of block to the fleeing suspect's path. This included establishing a roadblock with a patrol car or other obstruction, directing lights in the eyes of the approaching suspect, or deploying tire deflation devices. Figure 2 displays the trend in officer deaths related to this pursuit activity. As this figure reveals, there has *not* been a gradual decline in officer deaths of this nature. These types of officer deaths declined in the 1960s, dramatically rose again in the 1970s, and declined rapidly in the late 1980s and early 1990s. By the mid-1990s, these deaths were on a steep rise again and, after a brief dip, are continuing to rise today.

This unusual pattern may be explained by changes in the case law surrounding police pursuits, and the development of anti-pursuit technologies. Three landmark cases in the 1980s dramatically changed how roadblocks could be utilized during vehicle pursuits. First, in *Tennessee v. Garner* (1985), the U.S. Supreme Court took the first major step in defining the limits of police use of lethal force. One of many things that resulted from this case was the abolishment of the "fleeing felon rule" that had previously allowed the use of lethal force to prevent felons from escaping, regardless of the lack of imminent danger posed by the felon. This abolition, therefore, eliminated the practice of shooting at fleeing suspect vehicles (from a moving patrol car or a roadblock) in most cases. [1] The second case, *Jamieson v. Shaw* (1985), decided by the Fifth Circuit of the U.S. Court of Appeals, extended the decision in Garner to include other roadblock tactics that had a high likelihood of severely injuring or killing the fleeing suspect. In particular, this case suggested that placing a patrol car across the road on a blind curve and shining bright lights in the driver's eyes to prevent him or her from seeing the roadblock constituted an unreasonable seizure.

[2] In the third case, *Brower v. Inyo County* (1989), the U.S. Supreme Court also ruled that roadblock tactics that create a likelihood of death or injury to the fleeing suspect constituted an unreasonable use of force. In this case, officers had placed a semitruck completely across the highway around a curve, with patrol cars' headlights aimed to blind the fleeing driver on approach. [3]

These three court decisions and the influence they undoubtedly had on law enforcement agencies' pursuit practices may explain the tremendous decline in officer blocking deaths that began around 1985 and continued through the early 1990s. After 1985, roadblocks, if used at all, had to be constructed in a manner so that they would not cause injury to the fleeing suspect. Some of the pre-1985 officer deaths at roadblocks involved officers shooting at the fleeing driver from the roadblock, causing the driver to lose control and hit an officer or intentionally try to run down the firing officers. Others involved fleeing suspects being blinded by police lights, causing them to swerve and hit an officer. Still others involved officers off of the roadway who were hit when the suspect left the roadway in an attempt to go around a vehicle parked across the road. All three of these common scenarios were reduced dramatically by the restrictions placed on roadblocks by the U.S. federal courts. Fewer occurrences of these situations resulted in fewer officer deaths at roadblocks.

The steady resurgence of officer blocking activity deaths since the mid-1990s may be linked to the proliferation of tire deflation anti-pursuit devices. According to the U.S. Patents Office website, in the 1960s, no patents were filed for tire deflation devices. In the 1970s, two such patents were filed, and in the 1980s, seven patents were filed. In the 1990s, however, 19 new patents were filed, with another 24 filed in the first decade of the 2000s. [4] As the number and variety of these devices have increased, so have the number of officers killed attempting to deploy these devices. Almost all of the officers killed after 1995 while attempting some sort of blocking activity were killed while attempting to deploy tire deflation devices. Some were retrieving the devices from their trunks when rear-ended on the side of the road. Others were hit by the suspect vehicle or another citizen while deploying the devices, while still others were killed by patrol cars or other passing motorists as they attempted to retrieve the used devices from the road.

Traveling to Assist in the Pursuit

The last type of activity in which officers were engaged when killed during pursuits involved officers who were in fatal motor vehicle crashes while rushing in an attempt to either catch up to the pursuit or get ahead of the pursuit in order to establish a roadblock or deploy tire deflation devices. Between 1960 and 2011, 86 law enforcement officers died in this manner. Figure 3 reveals the pattern of these officer deaths since 1960.

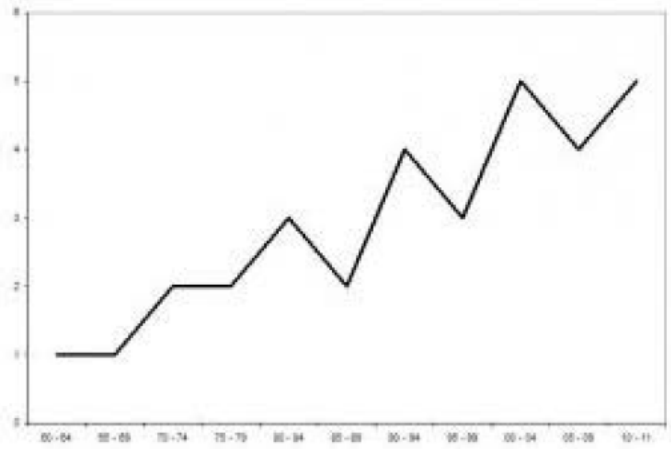


Figure 3. Officers killed while traveling to assist in the pursuit 1960-2011

As Figure 3 demonstrates, the number of officers killed in fatal auto crashes while traveling to assist in pursuits has been steadily increasing for several decades. In the 1960s, 13 officers died in this manner, but in the first decade of the 2000s, the number was 23, almost double the number of the first decade of the study. The exact reason for this steady increase is not completely clear. It may be a result of extensive media attention to vehicle pursuits today on news broadcasts and reality television shows, which glorify vehicle pursuits, possibly attracting officers to the excitement of a pursuit. It could also be an unintended consequence of the implementation of anti-pursuit technologies. More officers may be trying to get involved in the pursuit by establishing a blocking position with tire deflation devices. Finally, the expansion of radio communication capabilities and global positioning maps may have made more officers aware of the pursuit than was the case several decades ago. As more officers are aware of the pursuit, more officers try to get involved.

The authors have observed an increase in traffic collisions involving secondary officers responding to assist those in direct pursuit. When reviewing these collisions, it appeared that paralleling the pursuit had become commonplace. In some of the incidents reviewed, 20 or more police units paralleled a pursuit. The obvious safety issue with paralleling is the inherent danger associated with numerous emergency vehicles in close proximity traveling at high rates of speed while unaware of the others' locations.

The results of the present study raise the concern that the presence of the tire deflation devices in patrol cars may be resulting in an increase in the frequency and speeds associated with paralleling units. In fact, so great was the concern of one of the authors that, after reviewing the findings of this study, he directed all tire deflation devices

be removed from his agency's patrol cars. This decision was based upon the inability to support officers standing in roadways in close proximity to fleeing motorists traveling at high rates of speed, and the number of officers traveling at high rates of speed to get into position to deploy the devices was too great a risk to all concerned. The risks involved with the implementation of tire deflation devices demonstrate the need for the law enforcement profession to conduct evaluative research prior to implementing new technologies.

Implications for Policy and Practice

The results of this analysis of officer pursuit-related deaths may suggest the need for changes in police policies and practices. First, consideration should be given to expanding written departmental pursuit policies to include restrictions on the behaviors of officers assisting in pursuits. Just as many pursuit policies limit the number of officers or units that can participate in the pursuit, police executives should also consider restricting the number of officers who can engage in assisting with the pursuit. Limitations should be placed on how fast these assisting officers are allowed to travel, and, just like officers directly involved in the pursuit, they should be called off if traffic conditions make their travel unnecessarily dangerous.

Second, law enforcement agencies, in cooperation with tire deflation device manufacturers, should identify the safest and most effective tactics for establishing roadblocks and deploying these devices. By comparing tire-deflation device deployment incidents that resulted in deaths and injuries with deployments that were done safely, key differences may be identified that can lead to the development of best practices in the deployment of these devices. These evidence-based best practices can then be written into pursuit policies and incorporated into both academy and in-service training. It would also be beneficial to expedite the current research and experimentation into electronic vehicle kill switch technology that can remotely turn off the fleeing vehicle's engine, thus safely terminating the vehicle portion of the pursuit. Such technology is currently under development by several companies, but public pressure should be placed on these private companies to move more quickly to develop a model for practical field use.

Finally, to ensure officer buy-in with changes in tactics and written policies, street-level officers should be educated about the rising officer death rate from the deployment of tire deflation devices and traveling to assist in pursuits. Officers may exercise more caution when they realize that these activities are posing a greater risk to officer safety. Agencies can conduct after-action reviews to educate officers of the dangers they are posing to themselves and innocent motorists and pedestrians. Dash camera video footage from the assisting units, traffic camera footage, and in-car global positioning data can all be used in these after-action reviews to demonstrate to officers the dangers being posed by these activities.

Conclusion

The purpose of this study was to examine if they are being conducted in the safest manner. The natural tendency for police officers to over-respond during vehicle pursuits has long been an area of great concern for police administrators. Managing the fundamental desire of good cops everywhere to come to the aid of their peers remains an inherent challenge. Over the past several decades, considerable improvement in decision making has been demonstrated by officers and supervisors in direct pursuits. The information provided by this study reveals that the overriding concern today rests with the uncoordinated response of those coming to the aid of the officers in direct pursuit.

In spite of changes in technology, training, tactics, and policies designed to reduce the dangers vehicle pursuits pose for police officers, the annual number of officers killed *assisting* in pursuits has steadily been on the rise. Each decade, the number of officers killed while deploying tire-deflation devices or traveling to assist the pursuing officers increases. Street-level officers need to be informed of this growing danger, and better tactics and training need to be developed for the use of anti-pursuit technologies. Pursuit policies need to be expanded to include governing the behavior of officers assisting in pursuits. New anti-pursuit technologies need to be developed that would be safer for officers to deploy. Law enforcement is a dangerous profession, and every effort that can be made to improve safety should be made.

Notes:

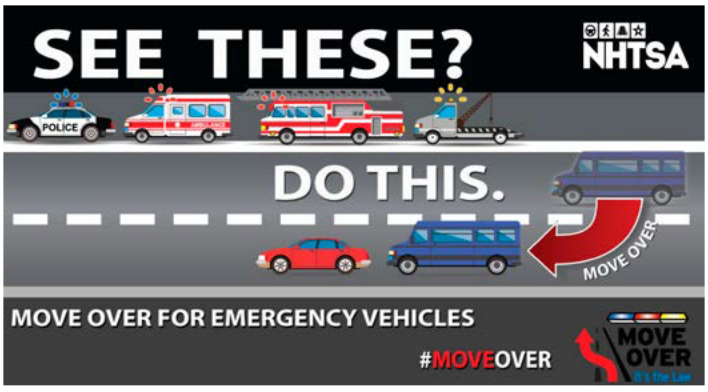
1. *Tennessee v. Garner*, 471 U.S. 1 (1985).
2. *Jamieson v. Shaw*, 776 F.2d 1048 (5th Cir. 1985).
3. *Brower v. Inyo County*, 489 U.S. 593 (1989).
4. U.S. Patent and Trademark Office, Patent Process—Search, http://www.uspto.gov/patents/process/search (accessed June 2, 2014).

Move Over Law

Law enforcement officers face various dangers in the performance of their duties. As highways become more congested and crashes become more complex to investigate, officers are facing even more dangerous circumstances. One of the most dangerous calls for service for officers is the various kinds of traffic-related incidents. Disabled and abandoned vehicles, traffic crashes, DUI, speed enforcement, and many other traffic duties place officers in harm's way, often on high speed interstates. There were 50 traffic-related officer deaths reported in 2018. This was a 9 percent increase from 2017. Traffic-related incidents one of the leading causes of death for on-duty law enforcement officers, fire, EMS, maintenance works, and tow/recovery professionals. [1]

Move Over Laws have now been enacted in all 50 States. While laws vary state to state, most require motorists traveling on controlled access highways with multiple lanes of traffic to move from the lane adjacent to stopped emergency or maintenance vehicles with lights activated. In addition, motorists must demonstrate due care to avoid colliding with such vehicles on all roadways.

As an example, the State of Colorado enacted a Move Over Law in 2005. The law states: "*On a highway with at least two adjacent lanes proceeding in the same direction on the same side of the highway where a stationary authorized emergency vehicle or stationary towing carrier vehicle is located, the driver of an approaching or passing vehicle shall proceed with due care and caution and yield the right-of-way by moving into a lane at least one moving lane apart from the stationary authorized emergency vehicle or stationary towing carrier vehicle...*" [2]



Source: University of Massachusetts Police Department

NHTSA, the IACP, State Highway Safety Offices, and other advocacy groups are aligned with law enforcement in an effort to better educate the public about Move Over Laws. Additionally, NHTSA, FHWA, and State Transportation Departments collaborate on Traffic Incident Management (TIM) training courses. The courses highlight the importance of Move Over concepts and raise the awareness of effective highway safety management and methods available to help improve the safety of motorists, crash victims, and emergency responders.

Notes:

1. National Law Enforcement Officers Memorial Fund (NLEOMF), *Preliminary 2017 Law Enforcement Officer Fatalities Report*, http://www.nleomf.org/facts/officer-fatalities-data/.
2. Move Over Laws.com, *Colorado Move Over Law*, http://www.moveoverlaws.com/colorado-move-over-law.htm (accessed May 31, 2017).

Officer Safety, Predictive Policing, and Community Relations



By: **Captain Arthur Combest,** Ohio State Highway Patrol, Columbus, Ohio

As an executive law enforcement leader, I think about officer safety every day. Hundreds of cadets enter through our academy doors each year to begin a career of public service, and I don't take my responsibility to them lightly. We train them to wear body armor to protect themselves from weapons. We teach them to wear safety belts in case of a crash. We also advise them that smart policing is safe policing.

"Smart policing" often translates to predictive or intelligence-led techniques that emphasize proactive efforts. Law enforcement agencies are sitting on treasure troves of data about the crime they address every day and tapping into that has revolutionized our ability to address the needs of our communities.

Police line of duty deaths in 2016 have spiked by 15 percent when compared to 2015.[1] With this in mind, law enforcement professionals are struggling to balance the need for officers to be out on the roads with the legitimate safety concerns that accompany visibility. The gut reaction is to pull back our proactive efforts. Though that protective instinct is understandable, we know our profession's future is not in reactive enforcement.

To recover our officers' confidence in proactive enforcement, our agencies need to rethink the traditional approach to officer safety. There is no one-size-fits-all solution. But we can start by expanding "smart" approaches to explicitly include community-police relations. We should also focus on transparency regarding proactive enforcement strategies, which we know

1 http://www.usatoday.com/story/news/nation/2016/11/02/ambush-style-killings-police-up-300/93155124/

ultimately make everyone safer. Our ability to do this will define officer safety in the 21st century environment.

We saw what's possible in July 2016, when hundreds of police officers and thousands of protesters descended upon Cleveland for the Republican National Convention. Law enforcement needed to reach civic and clergy leaders for assistance. Fortunately, networks of communication between the community and police were already in place. That community buy-in ahead of time was key to keeping the city and its people safe.

The story of that week could have been a dangerous clash with lasting damage as months of nationwide tension culminated in Cleveland. Instead, people who attended called it a block party.

Studies show the future of policing will emphasize these contacts more and more. When 200 police agencies were asked for their perspectives on the future of policing in 2012, 94 percent reported a current investment in community policing. It was the top response the surveyors received.[2]

Most police agencies understand that community safety is inextricably tied to officer safety. Officers can never completely control their environment. But they can contribute to a safer place with non-enforcement outreach efforts and by remembering every single interaction is an opportunity for a positive, lasting impression that improves officer safety.

This approach echoes the sentiment of the broken windows model, which suggests disorder in communities caused by less-severe crime leads residents to withdraw out of fear. That decrease in informal social control leaves a vacuum for serious crime to happen.[3] When police officers can encourage people to get outside and interact – through neighborhood walks, programs that reach children in friendly environments like schools, or participation in councils and groups that give people a space to gather and talk about their city's issues – we are investing in their safety as well as ours. It's about trust, and there isn't a part of it that isn't linked.

Another part of this effort to increase officer safety through community outreach is transparency. Transparency isn't about revealing confidential or personal information. It's about telling the public what we do and why we do it. This is increasingly important as our agencies invest in the kind of advanced technologies that make predictive policing possible.

Several news stories in 2016 highlighted public concerns related to new technology in policing. Use of start-ups like Geofeedia and Dataminr to monitor social media in targeted areas resulted in public backlash.[4] Seventeen civil rights and technology groups put out a joint statement that various predictive policing tools "supercharge" discrimination in minority communities.[5]

Whether or not civil liberties were violated is another discussion. The fact is community members are naturally suspicious of being treated like numbers, and too much reliance on technology without the human element of face-to-face conversation will breed distrust. That erodes any success we've had with community-police relations and officer safety, even though we know that intelligence-led policing will ultimately help everyone. It's taking two steps forward and one step back. We have to start a dialogue with our communities, and we have to translate that concern into visible and purposeful action.

Are we hosting or participating in face-to-face discussions with the community to explain the purpose of new initiatives and listening to their perspectives? While there, are we also explaining our officer safety concerns and how we all can work together?

Are we facilitating relationships with members of the media and pitching stories that dive into new technology and success stories? Are we sharing those stories on social media, where 6 out of 10 Americans now get their news?[6]

Are we viewing every single enforcement as an opportunity to make a good impression and prove that officers are there to help? Are we explaining to every law enforcement officer we employ how outreach is connected to officer safety, and are we giving them resources to prioritize those efforts?

These are worthwhile investments that have the potential to transform our interaction with the public and renew confidence in proactive policing. It'll lead to more trust, safer communities, and safer policing.

We are fortunate to work in a profession with colleagues who value the community and evidence-based approaches. More likely than not, your agency is already engaged with the community. Our end goal should be that a call to 911 feels like a call for help from a neighbor. Outreach efforts, transparency, and follow-up are essential to building these relationships.

2 http://www.policeforum.org/assets/docs/Free_Online_Documents/Leadership/future%20trends%20in%20policing%202014.pdf
3 http://cebcp.org/evidence-based-policing/what-works-in-policing/research-evidence-review/broken-windows-policing/
4 https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html?_r=0
5 http://www.cnsnews.com/news/article/barbara-hollingsworth/coalition-predictive-policing-supercharges-discrimination
6 http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/

This is a difficult, ongoing effort, but it is well worth it. The closer the bonds between police and the communities they serve, the safer we all are. That's what I want for law enforcement officers leaving our training academies and serving our communities.

Tactical Common Sense: Saving Lives with Seatbelts and Traffic Safety Vests

By: **Sergeant Joel Kuszynski,** Sheboygan, Wisconsin, Police Department

Adapted with permission from *"Tactical Common Sense: Saving Lives with Seatbelts and Traffic Safety Vests"*. The International Association of Chiefs of Police, (2016). Copyright held by the International Association of Chiefs of Police, 44 Canal Center Plaza, Suite 200, Alexandria, Virginia 22314 USA.

What would most police administrators or supervisors do if they learned of a simple, inexpensive piece of equipment that is proven to save lives? Would they hesitate to equip and train their personnel? What would many of them do if someone refused this piece of equipment?

There are two pieces of equipment that have been proven to save the lives of law enforcement officers, both of which are inexpensive and common. Most police leaders have likely already equipped their officers with them. Both of these items are constructed from simple nylon and, if used properly, will save lives: seatbelts and Class 2 or 3 ANSI/ISEA-approved vests. [1] Unfortunately, many officers are resistant to seatbelt and traffic vest use, claiming that they interfere with "good tactics."

Let's take a moment to talk about tactics. Merriam-Webster defines tactics as "the science and art of disposing and maneuvering forces in combat" and "the art or skill of employing available means to accomplish an end." [2] Police officers view tactics as team movements, angles, the use of firearms, and special training—all with the end goal of survival. No one would argue that good tactics and protective equipment aren't important to officer safety, and no police officer would intentionally go without body armor during a situation involving gunfire. However, many of those same officers choose not to wear seatbelts when driving a cruiser or an ANSI vest when standing in traffic. Why?

Police officers, especially those tactically minded, like gear. Ballistic vests, military-style carriers, rifle plates so light they float in water, communication systems, helmets, weapon lights... the list goes on and on. Most of this gear is black or camouflage, is expensive, and—most attractive of all—cool. Tactical terms are also cool: high/low, quick peek, hall boss, forward assault point, last cover, and concealment. The average seatbelt and traffic vest have little in common with other tactical gear with the exception of nylon webbing and hook and loop fasteners. They also don't share the cool factor; most of the time, they elicit the opposite reaction. Nonetheless, the lifesaving benefits of seatbelts and traffic vests are indisputable.

A study by the University of Michigan Transportation Research Institute found that an ANSI Class 2 or 3 vest increases the visibility of an officer in a simulated work zone from 125 feet to 891 feet. The average stopping distance of motor vehicles travelling between 35 MPH and 65 MPH is 159 to 425 feet. [3] Increasing officers' visibility along the roadway can literally save their lives.

Traffic-related deaths in the United States are the second leading cause of death for people ages 21–54. [4] Seatbelts are proven to save more lives in motor vehicle crashes than any other safety mechanism. [5] A head-on collision between vehicles traveling at 25 MPH is equivalent to driving a squad car into a brick wall at 50 MPH. Would anyone really be willing to do that without a seatbelt? Officers have no control over other vehicles on the roadway, and most officers are in a vehicle for the majority of their shifts. However, it appears that some do not realize the dangers of their most common function at work.

The arguments from officers who oppose the use of seatbelts or traffic vests tend to boil down to two primary concerns: "It takes too long to get a seatbelt off if I have to run after someone" and "My traffic vest makes me a target." Both sound like valid points, but, with some thought, they don't make sense. Of course, an officer shouldn't wear an ANSI traffic vest to an active shooting scene—the primary purpose of the vest, increased visibility, would be a significant drawback in this case. However, the vast majority of police officers drive a vehicle that is recognizable based on the model and markings. How can officers argue that, during routine activities, they wouldn't want the same visibility when out of their patrol vehicles?

Most states have a law similar to Wisconsin Statute 347.48 (2m) (dm), which exempts police officers from wearing seatbelts when "the operation of an authorized emergency vehicle by a law enforcement officer or other authorized operator under circumstances in which compliance could endanger the safety of the operator or another." [6] This is the excuse most often used by officers for not wearing seatbelts, but how often do most officers really encounter these situations? Do the risks of compliance outweigh the risks of not wearing seatbelts?

High-Visibility Education and Enforcement Pilot Program

As part of the continued focus on enhancing traffic safety and reducing fatal crashes across the United States, the IACP, the National Highway Traffic Safety Administration (NHTSA), the U.S. Department of Transportation, the Governors Highway Safety Association (GHSA), and other partners have created a High Visibility Education and Enforcement (HVEE) pilot program to enhance the Drive to Save Lives Campaign. Four states are currently participating in the program: Delaware, Maryland, North Carolina, and Wisconsin.

The pilot project focuses on using federal and state crash data and leveraging partnerships to respond to a particular traffic challenge in each area. Representatives from state and local law enforcement, state highway safety offices, and other public and private stakeholders partnered with IACP to look at NHTSA Fatality Analysis Reporting System (FARS) data and state crash data to determine each state's focus for the pilot.

Promising practices and lessons learned, including officer safety techniques, will be collected from each group. IACP will be producing and disseminating officer safety resources that will be useful for any officer engaged in motor vehicle enforcement. This type of traffic enforcement campaign is an opportunity for all departments to refresh officers' training and reinforce proper procedures and policies to ensure that officer safety remains a top priority.

Statistics may help officers understand why these two pieces of equipment are so important to their safety. According to the 2014 Federal Bureau of Investigation (FBI) statistics, 96 law enforcement officers were killed in the line of duty in 2014. Breaking the numbers down, 46 officers were killed with firearms; the other 45 were killed accidentally. Of the 45 officers killed accidentally, 28 were involved in automobile crashes and 6 were struck by vehicles. "Seatbelt usage was reported for 25 of the 28 officers killed in automobile collisions. Of these 25 officers, 15 were wearing seatbelts at the times of the accidents." No information was available on the use of ANSI traffic vests by those struck outside their cruisers. [7]

Taking a moment to analyze the numbers allows one to realize that accidental deaths are as common for police officers as are deaths by firearms. Between 1980 and 2008, 42 percent of the police officers killed in motor vehicle crashes were not wearing seatbelts. [8] Furthermore, a recent study by the California Commission on Peace Officer Standards and Training showed that nearly half of the police officers polled in California did not wear seatbelts. In contrast, the general U.S. public has a seatbelt usage that approaches 90 percent. [9]

There is an ethical aspect to this discussion, as well. Every state has either primary or secondary seatbelt laws that require citizens to wear them. Law enforcement officers are trusted with enforcing all laws. If an officer does not wear his or her seatbelt, can they ethically enforce the law? In addition, not wearing a seatbelt is often a policy violation. Policies are in place as a means of risk management. Are agencies effectively communicating these policies and their intent to their officers? Are police leaders willing to look beyond policy violations?

Law enforcement administrators should recognize that they have some control over these numbers. There are a number of different ways to increase seatbelt and safety vest use among officers. Possible approaches range from education to discipline, but the most effective method is creating cultural change. Implementing anticipatory change in an organization is certainly preferable to implementing reactive change resulting from the death of an officer. Roll call or shift briefing time is the perfect opportunity to reinforce the importance of safety gear, and those dialogues can be the gateway to cultural change in organizations. All lost officers are mourned, including those killed by violence and those killed in crashes, but people hesitate to ask whether or not an officer was wearing a seatbelt when killed in a crash. Most people don't wish to speak in accusatory terms when an officer loses his or her life, but can leaders and peers live with the possibility that an officer died as a result of not using proper safety gear because the importance of safety gear was not stressed or reinforced enough?

There is no question that every agency and leader make officer safety a priority. Likewise, the majority of officers also place a high priority on officer safety. The real question is whether the profession is dismissing the obvious when it comes to officer safety. If officers are as likely to die in a traffic incident as they are from a violent encounter, have agencies adequately focused their training efforts to reflect the reality of the risks? Do they spend as much time training officers in proper seatbelt usage and roadside work safety requirements as on the firing range? Agencies need to be willing to dedicate time to reinforcing seatbelt and safety vest use as part of tactical training. And, beyond training, police leaders must change their own traffic safety-related perspectives if they hope to change those of their officers.

David Kinaan, a former motorcycle sergeant in the California Highway Patrol, wrote a thought-provoking article titled "Courageous Conversations." He highlighted the need for police leaders to notice when officers are "taking shortcuts, or taking chances unnecessarily." He also noted that courage is needed by the person initiating the conversation, as well as the person listening to the conversation. In the article he asks, "If you don't say anything, who will?" [10] Leaders and peers must have the courage to start this conversation in their own agencies and with their own officers.

Ultimately, an agency is responsible for the actions of its officers. If the importance of seatbelts and traffic vests is not emphasized, officers may not take the issues seriously. If it is known that someone is not using proper safety equipment, steps need to be taken to correct the behavior, including discipline and remedial training as needed. The bottom line is that seatbelt and ANSI vest use is common sense. Officers know the dangers of their job, but they tend to focus all of their training on tactics. Law enforcement administrators need to dedicate more time and effort on the risks officers most commonly face on the job.

Notes:

1. Federal Highway Administration, "Pedestrian and Worker Safety," in *Manual on Uniform Traffic Control Devices for Streets and Highways* (2009), 564, 566, http://mutcd.fhwa.dot.gov/htm/2009/part6/part6d.htm#section6D03 (accessed January 21, 2016).
2. *Merriam-Webster*, s.v. "tactics."
3. University of Michigan Transportation Research Institute (UMTRI), "Illustration of Seeing Distances and Required Stopping Distances," 2 slides, https://www.usfa.fema.gov/downloads/pdf/saepedslide.pdf (accessed February 7, 2016).
4. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, "Leading Causes of Death," Web-based Injury Statistics Query and Reporting System (WISQARS), 2014, http://www.cdc.gov/injury/wisqars/leading_causes_death.html (accessed March 24, 2016).
5. National Highway Traffic Safety Administration, "Lives Saved in 2012 by Restraint Use and Minimum-Drinking-Age Laws," *Traffic Safety Facts* (November 2013), http://www-nrd.nhtsa.dot.gov/Pubs/811851.pdf (accessed February 9, 2016).
6. Safety Belts and Child Safety Restraint Systems, Wisconsin Stat. 347.48 (2m)(dm) (2001), https://docs.legis.wisconsin.gov/statutes/statutes/347/III/48 (accessed March 24, 2016).
7. U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services, "FBI Releases 2014 Statistics on Law Enforcement Officers Killed and Assaulted," press release, October 19, 2015, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2014-statistics-on-law-enforcement-officers-killed-and-assaulted (accessed January 21, 2016).
8. Eun Yong Noh, *Characteristics of Law Enforcement Officers' Fatalities in Motor Vehicle Crashes* (January 2011), 24, http://www-nrd.nhtsa.dot.gov/Pubs/811411.pdf (accessed February 7, 2016).
9. Tami Abdollah, "Not All Cops Use a Buckle," *Statesman Journal*, December 15, 2013, http://www.statesmanjournal.com/story/news/2013/12/16/not-all-cops-use-a-buckle/4036179 (accessed March 18, 2016.)
10. David Kinaan, "Courageous Conversations," *Law Officer* (April 2013), http://lawofficer.com/2013/04/30/courageous-conversations (accessed March 18, 2016).

CHAPTER 3: ALLOCATION, DEPLOYMENT AND EVALUATION OF TRAFFIC PERSONNEL

Police Allocation Manual (PAM)



By: **David Bradford,** *Executive Director,* Northwestern University Center for Public Safety

The *Police Allocation Manual (PAM)*, and *Police Allocation Manual User's Guide* were developed and field tested by Northwestern University Center for Public Safety under a contract (No. DTNH22-92-C-05051) issued by the National Highway Traffic Safety Administration, U.S. Department of Transportation. The author for the study was Dr. William Stenzel. The project was administered by the Office of Enforcement and Emergency Services.

There are three separate versions of The Police Allocation Manual (122 pages), one for state agencies, one for sheriff departments, and one for municipal departments. The Police Allocation Manual is designed to be used by law enforcement departments whose mission includes the delivery of patrol and traffic services. The Manual can be used to determine staffing levels for a traffic division with limited patrol coverage or for a patrol division with traffic responsibilities. The framework and rationale for the procedures presented in the Manual are the result of a distillation process that identified the "best" procedures currently in use by agencies throughout the United States, and then modified and blended those procedures into a comprehensive model for determining appropriate patrol staffing levels and deployment patterns. The procedures in PAM provide agencies with a logical and explicit format in which to frame requests for additional personnel and/or staff allocation. *The Police Allocation Manual* consists of four chapters and two appendixes:

- Chapter 1 provides a brief introduction to the purposes and uses of the Manual.
- Chapter 2 describes the PAM patrol staffing and allocation model.
- Chapter 3 contains eight worksheets, each with instructions that provide a step-by-step process for determining patrol staffing levels.
- Chapter 4 contains one worksheet for determining patrol staffing allocations over several geographic areas or time periods.
- Appendixes A and B contains worksheets that can be used as alternatives to the procedures presented in Section 5.2 in Chapter 3. Additional information about the PAM procedures can also be found in the companion document, *Police Allocation Manual User's Guide* (148 pages).

The Guide presents implementation, data definition, and data collection strategies used by the field test agencies. Also included in the Guide is a summary of key input values and numerical results obtained by the agencies that field tested the Manual.

The appendix materials in the Guide include:

- a list of the input data required to use the PAM model (Appendix A),
- a glossary of key terms and notation (Appendix B),
- a detailed example showing all nine worksheets in completed form (Appendix C),
- and derivations of all key formulas used in the model (Appendix D).

Law enforcement officers who are developing patrol staffing calculations for traffic safety services will find the information in the Manual to be very helpful. For additional information, contact the Northwestern University Center for Public Safety at nucps@northwestern.edu or toll free at 800-323-4011.

Using Traffic Safety Data to Drive Resource Allocation



By: **Jana R. Simpler,** *Former Director,* Delaware Office of Highway Safety and *Former Chair,* Governors Highway Safety Association

Law enforcement agencies are challenged every day with questions on how to best use their existing resources in a climate that is ever evolving. In the realm of traffic safety, support agencies such as the Office of Highway Safety can provide police agencies and law enforcement leaders with timely data to assist them in their decision making and resource allocation. Resource allocation in this day and age requires finesse. With no time, effort, or energy to waste, many law enforcement agencies are finding success by targeting limited resources by using crash data to drive decision making.

One of the most powerful resources law enforcement leaders generally should have at their fingertips is crash data, especially data specific to their jurisdiction. National crash data can be valuable in identifying trends and for making comparisons to support threat assessments about crashes and their causation at the macro level. The drawbacks related to national data are that it tends not to be as current or specific as state or local data and therefore not as valuable for making resource allocation decisions at the local level.

Law enforcement leaders may find their local and/or state crash data sets of greater value for making resource allocation decisions. Ultimately, all crashes are local, so the local data may provide greater clarity in the department's analysis of traffic safety issues. Because the relative sample population is far smaller, local data often provides greater insight regarding crash or injury causation, such as primary contributing factors, demographic details about the motorists involved, vehicle specifics, occupant protection use, problem intersections/locations, and levels and types of impairment. Armed with specifics about the types and locations of crashes, a chief, sheriff, or other operations officer can make informed decisions about how to allocate limited resources to address them.

A law enforcement agency's greatest assets are its human resources - especially its officers on patrol. Using the crash data to allocate resources allows an agency to more efficiently and effectively deploy these assets to improve traffic safety in their community. Officers can be directed to specific locations at specific times of the day/day of the week and even to look for specific violations. For example, directing safety restraint enforcement activities to an area where crashes are occurring in which drivers and/or passengers are unbelted typically leads to better compliance by motorists. Directed high visibility enforcement strategies have proven extremely effective at addressing a number of traffic safety issues, including safety restraint use, phone use and texting while driving, and impaired driving. Moreover, staffing strategies based upon crash data analyses are effective for general staffing, overtime traffic enforcement, and special details, such as saturation patrols.

Another related resource that law enforcement agencies manage is funding. With limited funds for traffic enforcement, crash data analysis can help identify an agency's traffic safety priorities and ensure that these limited funds are aligned with those priorities. This can facilitate decision making about where and when and for what target violation agencies deploy their officers. The analysis and subsequent targeted deployment can aid in driving the development of budgets related to the use of straight time and overtime funds.

Finally, there is a tremendous amount of evidence and commentary on the use of crime data to drive the use of staffing and allocate financial resources to address a certain problem. The same mentality for the use of crime data can easily be applied to the use of crash data to address crashes, serious injuries, and fatalities due to motor vehicle crashes. Targeting limited resources in a specific area, focusing on a specific violation as identified by careful crash analysis can reap dividends in the protection of the public and prevention of devastating crashes.

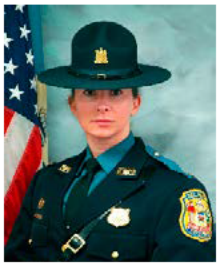
One model is the Data-Driven Approaches to Crime and Traffic Safety (DDACTS). DDACTS is an operational model for deploying law enforcement resources. This differs from traditional enforcement projects in that DDACTS is not meant to have a specific timeframe. DDACTS is a method of doing business. Operational deployment is based on data related to criminal incidents, traffic crashes, or other incidents causing social harm. The use of data is one of the primary elements of DDACTS, which is intended to "integrate location based crime and traffic crash data to establish effective and efficient methods for deploying law enforcement and other resources." [1]

Police leaders are always looking to work smarter, not harder. By using data to develop resource allocation models, leaders can pinpoint known traffic hot spots and provide more effective traffic safety practices for the community.

Notes:

1. Howard Hall, "Data-Driven Approaches to Crime and Traffic Safety — Its Application to Public Safety and Accreditation," *CALEA Update Magazine* (Issue 103).

The Changing of Culture as a Byproduct of the Delaware State Police's Implementation of the Stratified Model to Address Traffic Safety: The Pilot Study





By: **Captain Jennifer D. Griffin,** *Troop 1 Commander,* Delaware State Police and **Captain William D. Crotty,** *Director,* Delaware State Police Fusion Center and the Delaware Information and Analysis Center

Introduction

This article details the pilot study that was conducted by the Delaware State Police (DSP) on the implementation of the Stratified Model of Problem Solving, Analysis, and

Accountability (hereafter "Stratified Model"), which is an evidence-based practice to reduce incidents of criminal and traffic complaints using data driven analysis, while increasing accountability into police organizations day-to-day activities. The pilot study was conducted at Troop 1, a patrol troop in the northernmost region of the State of Delaware. This study officially started at Troop 1 on May 4, 2015. The goals of the pilot study were to:

- evaluate the usefulness of current data,
- evaluate and improve the quality and thoroughness of reports,
- improve responsiveness to the hot spots based on long term data analysis, as well as trends,
- ensure effective use of data by the Troop Administration and First Line Supervisors to develop and implement timely strategies,
- assess how officers respond to the new strategy,
- identify issues or obstacles and deal with them quickly,
- develop procedures to report outputs (productivity),
- develop means of communication to best convey information, data, and strategy,
- and most importantly, to increase accountability for Traffic issues across all levels of troop personnel from the captain to the newest trooper.

Agency

The Delaware State Police is a full-service law enforcement agency providing traffic and criminal enforcement along roadways and interstates, as well as patrol and investigative services in urban, suburban, and rural communities throughout the State of Delaware. With almost 800 troopers, the State Police is the largest police agency in the state and has primary jurisdiction statewide, while aiding numerous other law enforcement agencies.

Location/Participants

Troop 1, also known as the "First Troop in the First State" has been an icon, located at the top of Penny Hill since 1923. The 45-Troopers assigned to Troop 1 patrol an approximately 60-mile area, where diversity spans from Wilmington to Claymont, and Brandywine Hundred to Centreville. The patrol area also includes two interstate highways (I-95 & I-495), as well as the Concord Pike corridor, which has become a regional retail mecca, and the site of the world-wide headquarters for Astra Zeneca. During the pilot, Troop 1 was made up of four shifts, which included: one sergeant, one assistant, and eight patrol troopers per shift. The Troop also had a one trooper Retail Theft Unit (R.T.U.) and one Traffic Action Car (T.A.C.). The Troop Administration includes one traffic and one criminal lieutenant, who report directly to the captain, who is responsible for the overall implementation of the Stratified Model.

Stratified Model

The Stratified Model was developed by the pilot studies research partners, Drs. Rachel and Roberto Santos, who have been assisting law enforcement agencies in the United States and Canada over the last 10 years in implementing the model. This pilot study was one of the first times a state police agency in the United States implemented the model. The Stratified Model "provides a stratified structure that standardizes crime and traffic analysis, the problem-solving process, and accountability within a law enforcement agency while providing the flexibility to allow agencies to implement different evidence-based practices as they are deemed relevant for the unique nature of crime, traffic and environmental issues within a law enforcement jurisdiction." [1] The Stratified Model was selected due to its focus on using evidence-based practices to reduce incidents of criminal and traffic complaints, while using resources, both equipment and personnel, in the most efficient and effective manner, all the while embracing and enhancing community partnerships. For a comprehensive description of the Santos' Stratified Policing methodology as an example of a sustainability approach, please see the attached link from a presentation given at the Bureau of Justice 2013 Smart Policing conference (https://www.youtube.com/watch?v=R1G09KcAaqQ), or review *A Police Organization Model for Crime Reduction: Institutionalizing Problem Solving, Analysis, and Accountability.* Washington D.C.: Office of Community Oriented Policing Services.

Pilot study

A pilot study can be helpful as a "small-scale version or trial run in preparation for a major study." [2] A pilot study was employed because the Stratified Model was a major change from DSP's previously employed strategy of focusing primarily on solving crimes through intensive investigations, handing traffic crashes/issues after calls for service while reviewing statistics, versus ensuring responses were implemented effectively and efficiently. One of the major changes with the Stratified Model was the increased usage and reliance on data and analysis to formulate strategies to address and prevent additional incidents. There are five key factors to incorporate a structured approach to a pilot study. [3]

1. Plan and design the pilot study
2. Train personnel to accomplish change

3. Support and monitor pilot study
4. Evaluate pilot results
5. Make recommendations and improvements prior to agency wide implementation

Methodology

The Delaware State Police's method to execute this pilot study was structured around a simple three step process. The first step was an analysis focused on Data-Driven decision making via a comprehensive traffic study. The Delaware State Police utilized traditional hot-spot analysis of crash reporting data via the CrimeView system to identify geospatial density of crashes, day of the week and time of day frequency analysis, and analysis of the primary contributing behavior that led to the crash. CrimeView is computer software that allows for the mapping and organization of complex information from multiple databases into visualizations that reflect a snapshot of current activity. This analysis also allowed for the identification of locations and peak time periods where deployment could be most effective. Furthermore, the Delaware State Police also instituted a deployment time of 4-hours to coincide with these identified deployment areas.

The second step was to develop a specific traffic deployment strategy to target areas for crash reduction. This deployment strategy was formulated after an analysis of traffic data from the traffic study created by the Delaware State Police Crime Analysis Unit. Included in this strategy, was the identified responsibilities and accountability from the strategy development, to include collecting and reporting the results, which was performed by the Troop 1 Administration specifically reporting detailed metrics on the implementation of the strategy. The data points identified for this pilot were the following:

- Specific location
- Day of the week
- Time of the day
- Number of troopers assigned
- Number of hours dedicated in the target areas during target times
- Number of Traffic Summons/Citations for key crash contributing behaviors
- Total number of Summons/Citations - the focus was on the percentage (percent) of proactive enforcement in the hot spots, NOT the total number (#) of citations, or citations from crashes
- Number of crashes occurring during enforcement hours

The third step was the strict set of reporting periods of daily, weekly, and monthly reports based on the Stratified Policing Model process. Daily reporting occurred at the Troop level, where the Troop 1 Administration would report the strategy to include the specific deployment plan, and the outputs/productivity of the above data points. Weekly reporting occurred from both the Troop Administration and the Delaware State Police Crime Analysis unit. The weekly reporting from the Troop Administration consisted of aggregate reporting of the above data metrics, and the percentage obtainment of maximum deployment hours (i.e. 15 troopers covered 100 percent of the hot spot hours during the deployment times, and 550 /citations/ summons were issued, 500 of which were proactive/non-crash, on 480 separate operators). The weekly report from the Crime Analysis Unit would verify the specific metrics reported and the identification of data quality issues in reporting. Finally, monthly reporting from both the Troop Administration and Crime Analysis Unit summarized efforts and results. These monthly reports focused on aggregate reports of identified data metrics from the Troop Administration, while the Crime Analysis Unit provided a critical evaluation of deployment strategies/practices to validate which preformed behaviors of deployed Troopers optimized crash reduction. All the reports were shared with the Delaware State Police Executive Staff (Colonel, Lt. Colonel and Majors), Troop 1 Troopers, the County Investigative Units, and the Criminal Analysis Unit.

Rollout/Implementation of Stratified Model in the pilot study

Although a pilot study does not guarantee success when the strategy is fully implemented, it greatly increased the likelihood. To implement any type of change within a law enforcement agency, the first step should be to gather exhaustive information on the issue. The following is a brief chronological description of the process the DSP followed in developing the pilot study and then carrying it out:

- Gather exhaustive amounts of research and information on the Stratified Model
- Form a Stratified Model Committee
- Select a pilot location, in this case Troop 1
- Perform a Traffic and Crime Study of the pilot location, to provide data to drive decision and strategy creation
- Train Troop 1 Administration and First Line Supervisors, in this case Sergeants, on the Stratified Model, as well as their responsibilities/accountability
- Send explanatory emails and hold shift briefing meetings with all troopers to explain the model, implementation, goals, strategy, common language, and responsibilities/accountability

- Establish deadlines for reporting and communication
- Establish strict accountability guidelines to identify responsibilities at all levels

The first thing that had to be accomplished once the pilot site was identified, was to perform a comprehensive analysis of the troop's calls for service. This initial report established hot spots for traffic calls for service, which included crashes and traffic citation data. The analysis was performed by the Crime Analysis Unit and analyzed data for the prior year.

During 2014, Troop 1 investigated 2,856 traffic crashes. A geo-spatial analysis of the crashes clearly identified a hot spot of U.S. Route 202 and Interstate-95 which accounted for approximately 10 percent of all crashes in Troop 1 area. A report classification study revealed that reportable property damage crashes accounted for 67 percent of all crash investigations (1,928), Non-Reportable Crash investigations accounted for 17 percent of all crash investigations (503), Personal Injury Crashes accounted 14 percent of all Crash Investigations (416), and less than 1 percent were fatal crashes. Examination of the time of occurrence of these crashes revealed that 89 percent of all crashes occur between the hours of 0600 hours and 2100 hours, with 64 percent of all crashes occurring on the Interstate-95 between the hours of 0600-0800 hours. An examination of the primary contributing circumstances revealed the top three contributors to be Driver Inattention (19 percent), Following Too Closely (17 percent) and Careless Driving (11 percent). The utilization of the Stratified Model further focused the strategy and deployment for dealing with the traffic issues in the Troop 1 area.

Based on the enhanced data analysis, there were several initiatives that Troop 1 focused on to include:

- Increased enforcement during peak crash times and at hot spot locations;
- Increased proactive enforcement of crash contributing factors;
- Increased proactive DUI enforcement.

These were the top three traffic initiatives; thus, all traffic deployment tactics revolved around increasing productivity in these areas with a precise and targeted strategy. To reduce crashes based on the data, the Troop Administration's strategy was to have high presence and enforcement of crash contributing behaviors in the hot spot of Interstate-95 and U.S. Route 202 from the hours of 0600-1000. The second strategy was to increase proactive traffic enforcement as opposed to relying on troopers' enforcement of traffic violations *AFTER* crashes. And lastly, the third strategy was to increase DUI proactive production to engage the impaired driver before they crashed, as over 50 percent of all Troop 1 fatal crashes involved an impaired driver.

Results

During this pilot, Troop 1's first goal was to reduce traffic crashes in designated hot spots. To measure the success or failure of the pilot, the Troop 1 Administration examined the following data sets within the targeted area.

1. Geo-Spatial density changes to targeted area
2. Suppression of the frequency of crashes

Below is a representation of Geo-Spatial density changes to a targeted area. Table 1 is pre-pilot (January 1 - April 30, 2015), and Table 2 is post-pilot start (May 1 - August 30, 2015). Overall, looking at the post-pilot compared to the pre-pilot, it is evident that the increased enforcement decreased overall crashes. However, a deeper examination of the meaningfulness of these reductions from the focused 4-hour deployment by the Crime Analysis Unit found the following:

- Troop 1 successfully reduced crashes in the target area (U.S. Route 202 and Interstate-95) by 50 percent.
- The reduction of crashes in this targeted area also lead to a 30 percent reduction in the weekly complaint load for Troop 1.

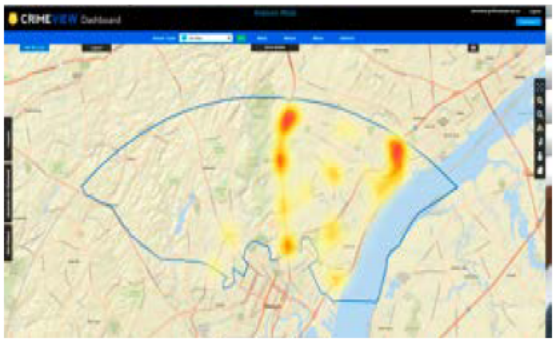


Table 1. Pre-pilot (Jan. 1 - April 30, 2015)

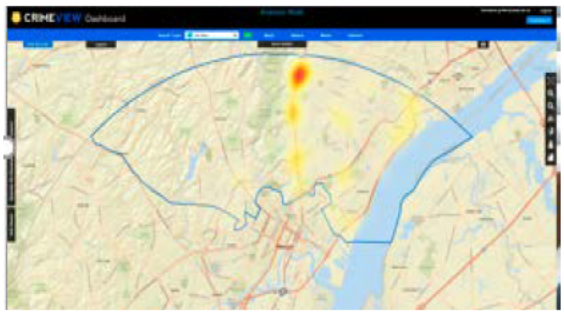


Table 2. Post-pilot start (May 1 - Aug. 30, 2015)

In regard to the second strategy of issuing proactive tickets in the hot spots, troopers were advised to focus enforcement during peak crash times at peak crash locations. Troopers' enforcement efforts were closely measured, and accountability was tracked to ensure that they were present and engaged in the hot spots during appropriate times. The strategized targeted enforcement directed troopers to specific locations, at specific times, to show both presence and perform meaningful enforcement of crash contributing behaviors. The goal was to be present in the hot spot during the strategic time to both deter and apprehend violators. A 100 percent coverage of the entire 4-hour block by one or more troopers was the goal set by the Troop Administration. Although this was not always achieved, troopers were covering over 80 percent of the time, with most shifts covering 90-100 percent of the 4-hour blocks. Thus, time present in the hot spot during the strategized time was monitored daily by all shifts. However, being present was not the only data point being tracked. Engagement and enforcement in the hot spots during peak times was also closely monitored and reported daily, weekly and monthly to track outputs. Troop 1 troopers consistently wrote between 85-98 percent of all proactive tickets in the hot spots. Proactive citations in the hot spots was a key data point and a goal to be maintained. On many days, Troopers wrote 100 percent of traffic citations in the hot spots, showing not only their engagement, but their dedication to the process, even if it meant that they got less citations than they would have written at a different location. This was also shared with the community and key stakeholders to show that troopers were issuing citations in high crash locations for crash contributing behaviors. The daily tracking of this data point reaffirmed the goal for Troopers to issue meaningful tickets for dangerous moving violations in locations identified as hot spots to reduce crashes and change crash contributing behaviors as opposed to just going out and getting numbers.

The following graphs are the pre-and post-frequency analysis of the targeted area to show that the increased enforcement during the 0600-1000 hours decreased crashes. During the pre-pilot period, there were more than 10 crashes between 0600-0700 hours, approximately 50 between both the times of 0700-0800 and 0800-0900 hours, and then 30 crashes between the hours of 0900-1000 hours. During the post-pilot period, crashes were reduced to less than 10 during the 0600-0700 hours, and less than 35 between both the times of 0700-0800 and 0800-0900 hours (30 percent reduction), and an almost equal amount of crashes during the 0900-1000 hour block. The reduction in crashes during the 4-hour period, which is historically a rush hour period for commuters, reduce the calls for services for Troopers to allow them to engage in proactive deterrence and enforcement, while

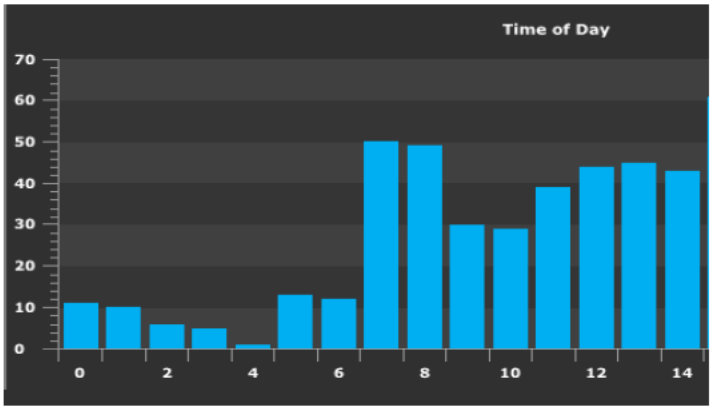


Table 3. Time of Day Pre-pilot (Jan. 1 - April 30, 2015)

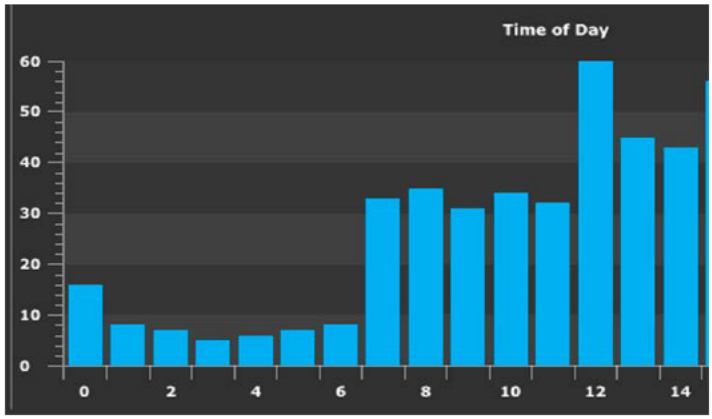


Table 4. Time of Day Post-pilot (May 1 - Aug. 30, 2015)

The last initiative was to increase proactive DUI enforcement, so that Troopers engaged the impaired motorists before they caused a crash and/or fatality. From May 1, 2014 to May 1, 2015, one full year prior to the pilot, Troop 1 troopers made 178 DUI arrests, 92 from crashes and 86 from proactive efforts. This resulted in 52 percent of DUI arrests from crashes and 48 percent from proactive enforcement. From May 1, 2015 to May 1, 2016, one full-year of the pilot study, Troop 1 Troopers made 243 DUI arrests, 91 from crashes and 152 from proactive efforts. This resulted in 37 percent of DUI arrests from crashes and 63 percent from proactive enforcement. Overall, there was a 15 percent increase when evaluating one year prior to the pilot to the first year of the pilot, and the overall number of DUI crashes decreased by 1 percent.

Lessons Learned and Conclusion

During and after the pilot study, there have been short- and long-term successes and cultural changes. In 2015, Troop 1 troopers worked to respond and adjust to the Stratified Model with its focus on the previously listed metrics and accountability. Most law enforcement leaders have heard the saying "There are two things that cops

hate most. The first is the way things are. And the second, is change." However, due to the successes experienced at Troop 1 in 2015 through the Stratified Model, there has been a cultural shift at all levels. The usage of accountability meetings and structured reporting not only provided timely data to base decisions on, but also provided timely updates on accountability. Prior to the pilot, troopers were more reactive to calls for service and less proactive in their efforts to decrease crashes. Throughout the process, engagement, effort, flexibility, and creativity were praised from the Troop Administration to the Executive Staff. Flexibility was a key component of the pilots' success, and failure wasn't seen as a negative, but as an opportunity to learn from a strategy and improve upon it. Due to the mentality that the strategies for handling a situation will change at any time depending on the data, the Troop Administration and troopers weren't afraid to try and fail because it viewed as part of the process to find what may or may not work. This allowed troopers at all levels the ability to take chances in their approach to resolving an issue.

One year after the pilot, the top three traffic initiatives continued to show success. In 2016, Troop 1 troopers again increased their proactive DUI enforcement by almost 20 percent. Increasing DUI production was critical to the Troop 1 traffic strategy as over 50 percent of DSP fatalities are DUI related; and by engaging the impaired driver prior to the crash, troopers are saving lives. Troopers, have also increased their proactive traffic enforcement in the hot spots, where most Troop 1 crashes occurred. On average, during the times of 0600-1000 hours between 90-95 percent of all proactive traffic citations were written in the hot spots, showing that troopers were enforcing traffic violations in those areas that are accounting for most crashes within the Troop area occur.

Although there are countless successes of the pilot study, and the full-implementation of the Stratified Model, there were challenges and obstacles that should be noted. First, with any change there is going to be apprehension and some resistance of the unknown. Agencies interested in moving to a Stratified Model with its data-driven focus need to take conscious steps to educate officers at all levels of the model, implementation, goals, strategy, common language, and responsibilities/accountability. Explaining the process through a variety of means (i.e. emails, PowerPoint presentations, informal and formal meetings) will not only ease fears and apprehension, but will also give officers input and buy-in to the process, as accountability and shared responsibilities is critical to the pilot's success. Secondly, make sure that other support units or groups understand the Stratified Model and their responsibilities and accountability in supporting the pilot location. Cultural change doesn't occur in a vacuum, and not ensuring other units not only understand the Model, but are held accountable for their responsibilities will surely undermine the pilot locations success. And lastly, remember that organizational culture isn't developed overnight, that it occurs over years, and in some cases generations. So, changing culture will take time, so do not lose hope when there are set backs or pushback.

Notes

1. Santos, Roberto G. & Rachel Boba Santos, Evidence-based policing, "What works" and Stratified Policing, "How to make it work," Translational Criminology 8 (September 2015): 20-22.
2. Polit, Denise .F., Cheryl Tatano Beck, & Bernadette P. Hungler, Essentials of nursing research: Methods, appraisals and utilization (5th. Ed.) Philadelphia: Lippincott, 2001.
3. Kasunic, M. (2004). SEPG Conference sponsored by the United States Department of Defense. Carnegie Mellon Software Engineering Institute (need proper citation)

Additional Information for the Bibliography of Resources

Boba, R. & Santos, R. (2015). *A Police Organization Model for Crime Reduction: Institutionalizing Problem Solving, Analysis, and Accountability.* Washington D.C.: Office of Community Oriented Policing Services. https://ric-zai-inc.com/Publications/cops-p208-pub.pdf

For more information on The OMEGA Group, Crimeview Dashboard System, go to http://www.theomegagroup.com/police/omega_dashboard_police.html

CHAPTER 4: CRASH INVESTIGATION

Every day, law enforcement officers provide a critical role in ensuring the safety of motorists on our roads. While education, enforcement, and engineering are all components to traffic safety, the thorough and sound investigation of a crash provides critical information in addressing driver behavior. Additionally, data from the police crash investigation may assist in developing effective enforcement and engineering countermeasures.

Police departments have developed effective data-driven strategies to address crime hot spots. Equally as important is the use of crash investigation data points to help departments allocate resources where repeat crashes occurred, where driving under the influence offenses are predominant and where the most egregious traffic violations seem to cause crashes.

While some police departments have had to limit their traffic enforcement functions in order to address what some might claim are more pressing violent crime trends, the fact remains that citizens continue to be very concerned about traffic crashes and traffic enforcement in their communities. While some agencies have focused more intently on violent crime, other progressive agencies have used evidence-based practices in applying crime fighting principles to simultaneously address traffic issues. At the heart of these solutions is the efforts of the officer on the scene of a crash in providing meticulous details and important data through a professional collision investigation.

Purposes of Investigating and Reporting Collisions

Ideally, a collision should be both *investigated* and *reported.* Police administrators must be mindful of the purposes of investigating and reporting. Law enforcement officers have multiple goals in their investigation of crashes. First, they are expected to protect the crash scene and those involved to ensure secondary collisions do not occur. Secondly, they also provide a written record, in the form of a crash report, of the facts of their investigation.

State laws outline specific requirements, however, in most states, any crash involving injury, death or a certain value of property damage, necessitate a police investigation and crash report. The ultimate purpose is to make our roads and highways safe. More immediate purposes are to combat criminal activity, promote safety, and just results in civil litigation. In very serious crashes, where a death results, criminal charges ranging from vehicular assault to homicide by automobile may follow. These complex investigations may lead to extensive and protracted investigative tactics and can involve the use of multiple police resources (i.e. specially trained fatal crash investigation personnel) as well as new technologies.

Detecting At-Fault Drivers

Although investigation frequently reveals who is primarily responsible for the collision, sometimes technical reconstruction is required. The at-fault driver can be charged with the violation(s) that caused the crash and, if convicted, can be punished or given remedial driver training. If the number of previous violations is sufficient for suspension of the driver's license, the individual's license can be suspended or revoked. By policy, police departments are tasked with holding at-fault drivers accountable for their driving which may have resulted in a serious collision.

Detecting Medically At-Risk Drivers.

A crash may be caused by a driver's physical or mental deterioration through illness or age. By working with state motor vehicle departments, the police investigator can request retesting to determine if that individual can still drive safely, if restrictions should be imposed, or if the driving privilege should be suspended or revoked. In the absence of a thorough crash investigation, a potentially dangerous driver could continue to drive without having the condition properly addressed.

Detecting Distracted Drivers

With the increase in the number of distracted driving crashes, law enforcement has an important role in attempting to determine the level of distraction in crashes. With greater awareness, training, and investigative techniques, officers can attempt to establish the level of distraction pre-crash. In the most severe cases and where the filing of serious criminal charges will result, officers know to preserve all evidence (i.e. cellphone or mobile device that has been identified) and to seek search warrants and/or prosecutorial advice on evidence preservation. Forensic analysis of a mobile device may be necessary to establish a "timeline of activity on the device" leading up to the crash. [1]

Apprehending Criminals

A vehicle involved in the crash may have been reported stolen or the operator may be involved in some other undetected criminal activity. A thorough crash investigation will establish a specific date and time of the crash. Significant unsolved crimes have been solved by investigators referring back to crash investigation reports which have placed a suspect at a crash scene. Without an investigation, these criminal acts might not be discovered, and offenders have an opportunity to reoffend.

Hit and Run Collisions

These collisions may require additional investigative steps to be taken in identifying the offending operator who may have already fled the scene of the crash. Police officers have successfully used sound police investigative skills, motor vehicle databases, reconstruction, witness interviews, and, increasingly, technologies such as highway cameras to arrest and prosecute offenders. Enhanced penalties, especially in very serious crashes, may result in criminal charges as well as the revocation of the license.

Use of Motor Vehicles to Cover Up Homicides

Vehicles have been used to carry out homicides, and to cover up homicides committed at locations far removed from the staged crash. These homicides may not have initially involved the motor vehicle as the primary weapon or homicide instrument.

In those cases where a death results and a motor vehicle is involved, police officers are encouraged to use state or regional specially-trained advanced crash investigation personnel to establish cause and the manner of death. In most cases, this will require extensive joint investigative effort with the local medical examiner or coroner.

Drivers without Licenses or Insurance Coverage

Another reason for conducting a comprehensive crash investigation is to establish the operator(s) possess the required license and liability insurance coverage. Police departments provide an important service to the community in detecting and seeking the prosecution of unlicensed and uninsured motorists. The collision investigation also provides critical information to insurance companies in assigning fault and compensating victims of crashes that may have resulted from a violation of state motor vehicle laws.

Defective Equipment

Equipment problems also cause collisions. Police crash investigators have the authority to inspect vehicles to ensure all equipment was functioning properly at the time of the crash. Investigators may also inspect and ensure all equipment meets the established design and equipment standards mandated by law. This is especially important for heavy commercial vehicles and buses whose weight can make them especially formidable in a crash. Crash investigations encompassing a thorough equipment inspection may lead to additional charges or the removal of the vehicle from the road.

Vehicle Design Defects

Crash investigations may uncover problems in the design of the vehicle or equipment. It may be prone to roll- over, have its fuel tank located where it is particularly vulnerable, or come equipped with tires susceptible to failure when under-inflated. With no policy requiring the investigation of every collision, such findings might never come to light or be recorded; inherently dangerous designs would never be corrected.

Roadway Defects

An investigation can reveal problems with the roadway design or conditions, or with traffic control devices. Such problems may have contributed to similar crashes in the past and continue, unless reported to the appropriate federal or state department of transportation.

Insurance Settlements

Unrelated to safety but important to those affected, an investigation can provide a means for civil litigation to help the aggrieved party recover just compensation and establish a basis for insurance companies to determine payments for property damage, personal injury, medical expenses, and disability. A perceptive, well-trained officer will detect crashes that have been staged to bilk insurance companies—a crime now of such proportions that it adds substantially to the cost of insurance for every motorist. A detailed crash report conducted in the field by a trained investigator can be an excellent tool in fighting fraud.

Collision Reporting

A qualified officer or civilian investigator should properly investigate every collision. It is also important to file a standard crash report for every collision. These reports allow the federal and state governments and law enforcement agencies to compile statistics to assess objectively the effectiveness of police traffic enforcement.

The concept of selective traffic law enforcement rests on data that show the violations that actually cause serious crashes, and the locations and times when they are most likely to occur.

Levels of Investigation

The severity and circumstances of a collision will determine the proper level of investigation. In their order of complexity, the levels are usually called *at-scene investigation, advanced (technical) investigation*, and *reconstruction.*

At-Scene Investigation

Basic to any collision is an at-scene investigation. Ideally, the first responding officer will conduct this and file a standard crash report.

The officer's first task is to make the collision scene safe and prevent a second crash. Traffic must be immediately redirected by means of patrol vehicles or other emergency vehicles, cones and/or flares. Next, the officer must care for the injured, summoning emergency personnel if needed, and then observe and record facts pertaining to the collision. These include all measurements, such as the length of tire marks and the final rest positions of collision vehicles and bodies from permanent reference points; the drag factor of the roadway surface; view obstructions; the condition of the collision vehicles, including lamps and tires; the condition of the roadway, traffic signs and signals; and the weather and environmental conditions (daylight or nighttime). A field sketch should be made to show the direction of travel of the vehicles and the location of all relevant objects.

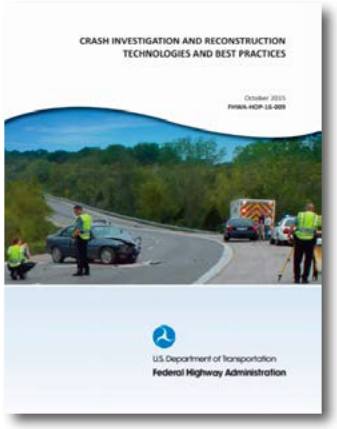
To document damage, the officer should photograph the vehicles and the collision scene. Finally, the officer should check all drivers for indications of impairment, interview all drivers and witnesses, and record their addresses and telephone numbers, as can is safe and reasonable to do so.

The at-scene investigation is concerned primarily with data gathering and recording. It may also involve some interpretation of the collected data. For example, from the skid mark measurements and the drag factor, the officer can calculate the minimum speed of the vehicle at the beginning of the skid.

Ideally, every officer should be qualified to conduct an at-scene investigation. By attending and successfully completing a state-approved course, an officer can become qualified to investigate crashes.

Emergence of Technology in Crash Investigation

In more complex cases or where significant criminal charges may result, investigators are more reliant upon emerging technology to aid their investigation. A comprehensive study was sponsored by the Federal Highway Administration in 2015. A report entitled "Crash Investigation and Reconstruction Technologies and Best Practices" was the culmination of this study. It provides information about traffic crash reconstruction technology investigators are using in the field as well as other evolving and promising innovative equipment for crash investigation and reconstruction. [2]



The technologies detailed in this report are becoming much more prevalent in their use by investigators. Global positioning systems, three-dimensional laser scanning, unmanned aerial systems (drones), among others, are all helping investigators to provide more precise investigative finding while also enabling roadways to be cleared of crashes and the traffic flow to be restored more quickly. This reduces the length of time that emergency response workers are exposed to traffic hazards at the scene.

Advanced (Technical) Investigation

Whereas an at-scene investigation should be conducted for *every* collision, an advanced investigation is undertaken whenever the data obtained at the at-scene level is considered insufficient to complete the investigation. The purpose of the advanced investigation is to collect additional data for determining the charges to be brought against one or more of the individuals involved, for litigation reasons, or for laying the foundation for the next level of investigation—re-construction.

Unlike the at-scene investigation, which is initiated immediately or as soon as practicable after the collision, the advanced investigation may take place at a later time. Data, including that from the at-scene investigation, will be interpreted, as well as collected. Since much of the evidence at the scene may already have disappeared, the advanced investigation may depend heavily on the completeness and accuracy of the data recorded in the at-scene investigation.

The same officer who conducted the at-scene investigation, if trained and qualified, may conduct the advanced investigation. This officer is expected:

- To determine the drag factor of the skid surface(s) and the minimum initial speed of each vehicle (unless already calculated in the at-scene investigation);
- To determine time-distance relationships and solve momentum problems;

- To match marks on the roadway with the parts on the vehicle causing this damage, to determine the point of impact;
- To determine what is impact damage to the vehicle and what is contact damage;
- To match the damaged areas of the vehicles to determine the principal direction of force (PDOF);
- To correlate injuries with the parts of the vehicle impacted by the occupants (occupant kinematics);
- To determine if headlamps and other lamps were ON or OFF at impact;
- To determine if any fire damage occurred before or after impact;
- To determine if a mechanical or electrical failure contributed to the crash (this may require the help of a specialist); and
- To prepare a scale drawing of the scene from measurements and notes made at the scene.

Officers can receive advanced investigation training by successfully completing a POST-approved course. The length of this training is up to 80 hours, and includes classroom instruction and hands-on activities. A prerequisite is usually the completion of a basic collision investigation course, such as at-scene investigation, or several years' practical experience in at-scene investigation.

Collision Reconstruction

Reconstruction is the highest of the three major levels of investigation, and is usually undertaken only in support of litigation or research. Its main purpose is to determine *how* the collision occurred. It deals primarily with direct and immediate causes of the crash. These frequently entail behavioral errors on the part of the drivers.

The findings are mostly objective, supported by the facts uncovered or determined by investigation at any of the three levels. The purpose may be extended to attempt a determination of *why* the collision happened (called "cause analysis" and sometimes regarded as a separate and even higher level of investigation). This phase looks at all the circumstances of the crash in order to identify the probable and possible contributing factors.

The findings are to some extent speculative. Take, for example, a case where two vehicles crash head-on. The *direct* cause is that one vehicle suddenly crossed the centerline and encroached on the opposite travel lane, placing this vehicle in the path of an oncoming vehicle. The probable *indirect* cause may be that the driver of the encroaching vehicle fell asleep, inasmuch as the collision occurred at 3:00 A.M., and the driver had been driving continuously since the previous noon.

Reconstruction expands on all the principles of at-scene and advanced investigation. In addition, it includes impulse—or the force exerted by each vehicle upon the other—and energy loss through crush—or the extent of deformation of the vehicle caused by the impulse. It may involve experiments to ascertain performance and other capabilities of the vehicle, or to determine driver and pedestrian behavior. Reconstruction entails assembling all the technical data required to build a case for court.

Among the duties of the reconstructionist are the following:

- Cooperating closely with the attorney, if litigation is involved;
- Interpreting photos, information contained in field notes, and all other recorded data from the at-scene and advanced investigations;
- Using photogrammetry to determine distances between objects and location of objects;
- Matching paint, glass and vehicle parts found at the scene to the vehicle being sought after its driver fled;
- Determining who was the driver of each vehicle;
- Determining occupant movement (occupant kinematics) and how injuries were received;
- Checking all calculations made previously and performing any additional calculations required; and
- As needed for the courtroom presentation, preparing scale diagrams of the scene—often via specialized computer-aided diagramming software—showing vehicle and body positions, time-distance relationships, and momentum vectors.

Although a reconstructionist usually has greater depth of knowledge and broader experience than an investigator qualified only in at-scene or advanced investigations, and can make more inferences from existing data, he is very dependent on the thoroughness and quality of the investigations conducted at the scene, and may have to work largely with the evidence that has been preserved and recorded by the officers who initially responded to the scene.

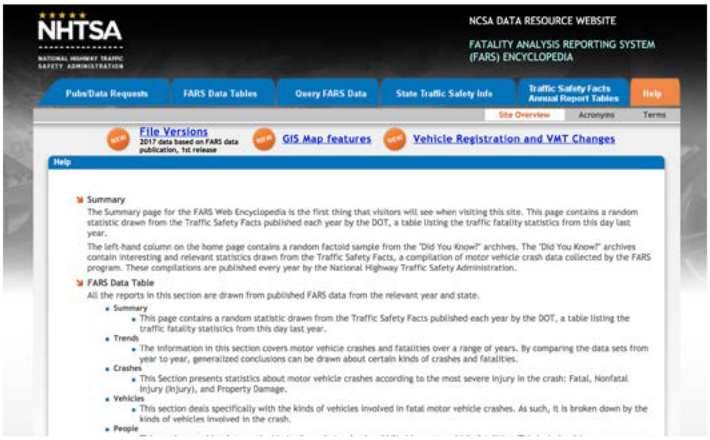
Officers can receive training in reconstruction by attending a POST-approved course of up to 80 hours in length. Such a course combines classroom instruction with hands-on activities. The pre- requisite is usually successful completion of a state-approved course in advanced (technical) investigation. More advanced and specialized

crash reconstruction training is typically conducted a state police academies by highly-trained senior investigators. Organizations such as the Institute of Police Technology and Management offer the "At-Scene Traffic Crash/Traffic Homicide Investigation" course and an "Advanced Traffic Crash Investigation" course, among others. (To learn more about these courses, see: http://iptm.unf.edu/)

Using Data to Better Understand Crashes: The Fatality Analysis Reporting System (FARS)

Police departments have become increasingly more skilled at using traffic crash data to address "hot spots" by deploying high-visibility enforcement in identified problem locations. As data has become more important to the efforts in analyzing crashes and causation factors, the need for comprehensive crash reporting by police officers is underscored.

NHTSA developed the Fatality Analysis Reporting System (FARS) in 1975 to assist the traffic safety community in identifying traffic safety problems and to evaluate both motor vehicle safety standards and highway safety initiatives. FARS maintains, analyzes, and provides access to data from motor vehicle crashes in the United States that occur on a public roadway and involve a fatality. NHTSA collects and tabulates data on fatal crashes from all 50 states, the District of Columbia, and Puerto Rico. NHTSA contracts with each state government to provide information on fatal crashes within the state. [3]



Source: NHTSA, FARS Encyclopedia site. https://www-fars.nhtsa.dot.gov/Help/Help.aspx

States also maintain their own traffic crash and highway safety data and some states have a Traffic Records Coordinating Committee (TRCC). The Governors Highway Safety Association, working with its State Highway Safety Offices (SHSOs) and NHTSA are involved in many efforts to ensure traffic crash data is standardized and can be used in the planning of effective highway safety programs. [4]

Additionally, the Model Minimum Uniform Crash Criteria (MMUCC) is another data set that law enforcement officers can use to help with planning effective highway safety strategies. The MMUCC is a voluntary minimum, standardized data set for describing motor vehicle crashes and the vehicles, persons and environment involved. The Guideline is designed to generate the information necessary to improve highway safety within each state and throughout the U.S. This data set, originally published in the MMUCC Guideline, 1st Edition (1998), has been revised three times, most recently in the 4th Edition (2012), in response to emerging highway safety issues. The 5th Edition is scheduled for a summer 2017 release. [5]

The Federal Highway Administration (FHWA), through its Office of Safety Programs, uses "safety data to identify those areas with the greatest need for improvement because understanding the most prevalent safety problems on our roadways is the first step to solving them. The FHWA Office of Safety's Roadway Safety Data Dashboard provides graphical presentations of data elements that characterize fatal crashes on U.S. public roadways. These elements include FHWA and NHTSA definitions of fatality type, collision type, collision location, and type of person involved in the fatal crash. All of these elements can be viewed and compared at the national, State, regional, or MPO level." To access the dashboard, click on https://rspcb.safety.fhwa.dot.gov/Dashboard/Default.aspx. [6]

Notes:

1. Horsman, Graeme, and Lynne R. Conniss. "Investigating Evidence of Mobile Phone Usage by Drivers in Road Traffic Accidents". *Digital Investigation* 12 (2015): S30-S37. doi:10.1016/j.diin.2015.01.008.
2. Federal highway administration. *Crash Investigation and Reconstruction Technologies and Best Practices*. Washington, DC, 2015.
3. "PIA - Fatality Analysis Reporting System". *US Department of Transportation*, accessed September 3, 2017, https://www.transportation.gov/individuals/privacy/pia-fatality-analysis-reporting-system.
4. "Traffic Records | GHSA". *Ghsa.Org*, accessed September 3, 2017, http://www.ghsa.org/issues/traffic-records.
5. "Model Minimum Uniform Crash Criteria (MMUCC)". *US Department of Transportation*, accessed September 3, 2017. https://www.transportation.gov/government/traffic-records/model-minimum-uniform-crash-criteria-mmucc-0.
6. "Facts & Statistics - Safety | Federal Highway Administration". *Safety.Fhwa.Dot.Gov*, accessed September 3, 2017. https://safety.fhwa.dot.gov/facts_stats/.

CHAPTER 5: COMMERCIAL VEHICLES AND HAZARDOUS MATERIALS REGULATION

U.S. Department of Transportation

Federal Motor Carrier Safety Administration

As the lead federal government agency responsible for regulating and providing safety oversight of Commercial Motor Vehicles (CMV) in the United States, the Federal Motor Carrier Safety Administration's (FMCSA) mission is to reduce crashes, injuries, and fatalities involving large trucks and buses.

FMCSA was established on January 1, 2000, pursuant to the Motor Carrier Safety Improvement Act of 1999 (Public Law 106–159). Prior to this legislation, motor carrier safety responsibilities were under the jurisdiction of the Federal Highway Administration. FMCSA resources and programs are focused on and support its mission through education, regulation, enforcement, research, and innovative technology, thereby achieving a safer transportation environment. Additionally, FMCSA is responsible for ensuring that commercial vehicles comply with all Federal Motor Carrier Safety Regulations (FMCSR) and Hazardous Materials Regulations (HMR). Further, to accomplish these activities effectively, FMCSA works closely with Federal, State, and local enforcement agencies, the motor carrier industry, highway safety organizations, and the public.

The agency is guided by four core values:

- **Integrity.** We uphold the highest standards of equality, integrity, and ethical behavior. Through our actions, we earn the respect and trust of our peers, partners, customers, and the American people.
- **Knowledge.** We seek new ways to accomplish our responsibilities and achieve extraordinary results by delivering creative, forward-looking, and data-driven solutions in advancing our mission.
- **Collaboration.** We work as a team, furthering our goals and strategies by valuing the commitment and contributions of our many partners and stakeholders to achieve mission success.
- **Excellence.** We strive for excellence and seek to provide the highest level of service by embracing our mission with the utmost energy and enthusiasm.

We Are FMCSA Brochure.pdf

CMVs play a significant role in moving our nation's economy. They transport volumes of goods and carry thousands of passengers across the country every day. Every mode of transportation moves freight, but trucking is the primary mode of freight travel.

At the same time, CMVs pose unique safety and regulatory challenges due to their size, weight, and unique operation—from wide turns and massive blind spots, to transportation of hazardous materials.

That's why FMCSA asks everyone to be a partner in truck and bus safety.

FMCSA partners with industry, safety advocates, and state and local governments to keep our nation's roadways safe. Approximately 1,100 dedicated FMCSA employees across the country work diligently every day to improve CMV safety by preventing large truck and bus crashes and saving lives.

Our Roads, Our Responsibility

Large trucks and buses maneuver very differently than passenger vehicles. The *Our Roads, Our Responsibility* campaign empowers all drivers to be aware of those differences and make simple adjustments to help keep the roads safer for everyone.

Learn more about the Our Roads, Our Responsibility campaign.

Grants and Financial Assistance

FMCSA safety grant funding opportunities are primarily available to state and local government agencies in the 50 U.S. states, the District of Columbia, Puerto Rico, Northern Mariana Islands, American Samoa, Guam, and the US Virgin Islands. Applicants for FMCSA funding opportunities should be working on commercial motor vehicle safety activities and should demonstrate a capacity to work with highway traffic safety stakeholders which may include, but are not limited to, state and local law enforcement agencies, state departments of public safety, departments of transportation, state traffic records coordinating committees, associations that focus on commercial motor vehicle safety and training issues, and other industry stakeholders.

FMCSA State and local government grantees often work in conjunction with for-profit and nonprofit organizations including public and private institutions of higher education, businesses and independent contractor consultants. Specific eligibility for each of the FMCSA safety grant funding opportunities is defined below.

Commercial Driver License (CDL) Program Implementation Grant

Eligible Applicants: The state agency designated as the primary driver licensing agency responsible for the development, implementation and maintenance of the CDL program or State agencies local governments, or other persons for high priority activities or emerging issues as identified by the Secretary of Transportation. Learn more about the CDL Program Implementation Grant.

CMV Operator Safety Training Grant

Eligible Applicants: State or local governments; accredited post-secondary educational institutions (public or private) including colleges, universities, vocational / technical schools and truck-driver training schools. Primary funding priority is given to regional or multi-State educational or not-for-profit associations that recruit and train current and former members of the United States Armed Forces (including National Guard members and Reservists) and their spouses to receive training to transition to the CMV operation industry. Learn more about the CMV Operator Safety Training Grant.

Motor Carrier Safety Assistance Program (MCSAP) Grant

The Motor Carrier Safety Assistance Program (MCSAP) is a Federal formula grant program that provides financial assistance to States, including the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, American Samoa, Guam, and the U.S. Virgin Islands to reduce the number and severity of crashes and hazardous material incidents involving commercial motor vehicles (CMVs). Specifically, only the State lead agency (as designated by the Governor) is eligible to apply for MCSAP grant funding. Learn more about the MCSAP Grant.

High Priority Grant

High Priority is a Federal competitive grant program which provides financial assistance to States, local governments, federally recognized Indian tribes, other political jurisdictions as necessary, and other persons to carry out high priority activities and projects that augment motor carrier safety activities and projects:

1. To carry out activities and projects that augment motor carrier safety;
2. To advance the technological capability and promote the deployment of intelligent transportation system applications for CMV operations, including CMV, commercial driver, and carrier-specific information systems/networks; and to support and maintain CMV information systems and networks.

Learn more about the High Priority Grant.

Regulations

Regulations issued by FMCSA are published in the Federal Register and compiled in the U.S. Code of Federal Regulations (CFR). Copies of appropriate volumes of the CFR in book format may be purchased from the Superintendent of Documents, U.S. Government Printing Office, or examined at many libraries. The CFR may also be viewed online.

Search

Search FMCSA Regulations and Interpretations - 49 CFR Parts 300-399

Search HM Regulations - 49 CFR Parts 100-177

Search HM Regulations - 49 CFR Parts 178-180

Unified Registration System

FMCSA monitors and ensures compliance with regulations governing both safety (all carriers) and commerce (for-hire carriers). Companies may find they are subject to both registration requirements (USDOT Number and MC Number) or either one separately. To determine the need to apply for a US DOT number, click here. Learn more about URS.

Commercial Driver's License Program

Driving a Commercial Motor Vehicle (CMV) requires a higher level of knowledge, experience, skills, and physical abilities than that required to drive a non-commercial vehicle. In order to obtain a Commercial Driver's License (CDL), an applicant must pass both skills and knowledge testing geared to these higher standards. Additionally CDL holders are held to a higher standard when operating any type of motor vehicle on public roads. Serious traffic violations committed by a CDL holder can affect their ability to maintain their CDL certification.

Licensing

Driving a commercial motor vehicle is a big responsibility. It requires special skills and knowledge. Most drivers must obtain a commercial driver's license (CDL) through their home State (it is illegal to have a license from more than one State). In addition, special endorsements may be required if you or your company drivers will be driving any of the following vehicles:

- a truck with double or triple trailers
- a truck with a tank

- a truck carrying hazardous materials
- a passenger vehicle

Learn more about the Commercial Driver's License Program.

Hazardous Materials

FMCSA's mission includes reducing the number of transportation incidents that involve hazardous materials and could potentially harm the public and the environment. Developing programs to accomplish these goals and increase the safety of hazardous material transportation is the responsibility of the FMCSA Hazardous Materials (HM) Program. Learn more about Hazardous Materials Transportation.

Protect Your Move

Planning to move? FMCSA can help protect your life's memories and move with confidence. Our "Ready to Move" brochure and checklist is a handy tool to help you prepare for your move, and understand what you will need to know and do during each phase of your moving process. Explore the sections below to learn more.

Get Started

Learn About Moving Fraud

Find out what you need to know about moving fraud so you can plan your move with confidence.

Let's Go

Research Your Mover

When you move, there's plenty to worry about. Your mover shouldn't be one of them.

Get Started

File a Moving Fraud Complaint

Trouble with your move? Your complaint may help prevent others from becoming victims of moving fraud.

Look Before You Book

Cost effective... energy-efficient... comfortable... It's little wonder that bus travel is growing in popularity. And, overall, buses are one of the safest passenger options.

But even one crash is too many – particularly if you, a loved one, or your travel group is affected.

When planning a trip, exciting destinations and fun activities may be top of mind. Business or necessary personal bus travel may put the focus on convenience and cost.

But safety should always be the highest priority...

Wherever you're going, make sure the bus company that's bringing you there is safe. Check out the company's safety record and always Look Before You Book!

Contact Us

Headquarters

Federal Motor Carrier Safety Administration
United States Department of Transportation
1200 New Jersey Avenue SE
Washington, DC 20590

Field Offices & Service Centers

- Field Office Contact Information

Contact	Number
FMCSA Information Line ▪ U.S. DOT Numbers ▪ Status of DOT Numbers ▪ Operating Authority Information ▪ Safety Ratings ▪ Licensing Information ▪ Insurance Information ▪ Email ▪ Chat	1-800-832-5660
Consumer Complaints ▪ Household Goods ▪ Passenger Carrier (Motorcoach/Bus/Van) ▪ Hazardous Materials ▪ Safety ▪ Driver	1-888-DOT-SAFT 1-888-368-7238
Federal Relay Service for TTY	1-800-877-8339
Share the Road Safely	202-493-0472
NHTSA Hotline Number	1-888-DASH-2-DOT 1-888-327-4236

CHAPTER 6: DRIVER LICENSING SYSTEM

The Driver Licensing System



By: **Brian Ursino,** *Director of Law Enforcement,* American Association of Motor Vehicle Administrators (AAMVA)

Motor vehicle administrators of the U.S. states and Canadian provinces generally are responsible for issuing driver licenses. As well as serving as the *de facto* identification document of choice, the state-issued driver license also is used for:

- The verification and identification of persons who are driving motor vehicles;
- The operation of a secure license testing system which provides separate knowledge and skill tests for various types of vehicles, such as motorcycles, passenger vehicles, and commercial vehicles;
- Managing a pointer system targeting unsafe drivers for license suspension or revocation to remove hazardous drivers from the roads;
- Managing the Commercial Driver License Information System (CDLIS) pointer to ensure that commercial drivers have one driver record and one license; and
- Identifying and tracking traffic violators through the court system and preventing persons from defaulting on traffic citations.
- Responsible for accessing various Federal databases (i.e. Systematic Alien Verification for Entitlements (SAVE) and Social Security Numbers (SSN) via SSOLV, etc.)

The License as a Positive Identifier

When first issued, driver licenses were intended to verify that the holder complied with the regulations associated with vehicle operation and the privilege to drive.

A driver license database typically contains a variety of information, including some—but not always all—of the following: full name, date of birth, date of issue, date of expiry customer identifier, document discriminator, portrait, signature, cardholder address, vehicle classifications, endorsements, restrictions, sex, height, and eye color.

The DL/ID card has become the identity document of choice for satisfying: evidence of the privilege to drive, identification, age verification, address/residence verification, and automated administrative processing.

The state and provincial agencies issuing driver licenses are finding that better identity proofing and vetting of applicants is very challenging due to the absence of better initial identification systems. Currently, the verification of a U.S. birth certificate is less than optimal for identification purposes.

Motor vehicle administrators never sought to have driver's licenses serve as a national identification. However, when photographs were added to licenses to aid in positive identification and to reduce fraud, their usefulness for other purposes soon became apparent. Today, it is virtually impossible to cash a check, to board a commercial aircraft, to obtain government benefits, to access certain restricted areas, or to rent a car without presenting a valid license. In fact, many states and provinces have now passed laws that require motor vehicle agencies to issue "non-driver's photo identification cards" to persons who do not drive.

All states and most provinces are now using a digital photo method (versus a printed photo that is then affixed), which provides more effective physical security and permits photographic information to be transmitted via computer to police officers in the field.

These documents offer advantages over instant photo technology. Central electronic image storage makes access to the pictures and information much easier. Digital imaging has eliminated some of the fraudulent practices that plagued previous affixed photo approaches. Multiple driver's licenses, held by the same or different people, are more difficult to obtain, if the licensing authority takes the time to compare the appearance of the person applying for a duplicate license to the digital image of the original applicant.

Auditing of the driver's license production procedure also helps to eliminate abuse by individuals who create fraudulent licenses used in check and credit card fraud, in drug trafficking, in underage drinking, in tobacco usage and, in illegal immigration.

The implications for law enforcement go far beyond these obvious benefits. With a central image database of every driver in a state, the public safety community has a ready-made storehouse of photos that may be available to law enforcement except for those jurisdictions where privacy laws prevent such usage. The public safety community, particularly law enforcement, should be continually alert to legislation that limits and/or precludes the transmission to a police officer of the digital image driver's license and pertinent information.

After the Pentagon and World Trade Center terrorist attacks, concerns arose in the United States over the ease with which undocumented immigrants could obtain driver's licenses by using counterfeit supporting documents. In fact, several of the 9/11 terrorists had obtained multiple driver's licenses from various jurisdictions and had driven extensively throughout the Eastern seaboard and the Midwest, apparently scouting potential targets for attack.

Over the past several years, there has been widespread criticism of loopholes in the system of issuing driver's licenses and a call for national standardization of driver's license formats and data elements. Responding to such criticism, some oppose such standardization for fear that it would lead to some sort of "national identity card" that people would be required to display, similar to practices in some totalitarian nations.

Another major problem is the use of fraudulent driver's licenses by minors to purchase alcoholic beverages. A number of states have addressed this problem through the use of special licenses, or the addition of identifying features to the licenses of persons under the age of 21 years, so law enforcement, bartenders and package store employees can readily identify them. For example, many states now issue a vertical driver's license/ID card valid for persons under 21 years old.

Strategies to prevent counterfeiting and fraud include the use of biometrics, micro-printing, digital watermarks, digital photo overlays, and optical varying devices (typically holograms). Many states include additional security features in their documents that are not publicized outside their agencies. Other strategies include attacking the problem at the source by training license issuing agents and examiners to better spot phony supporting documents, such as birth and baptismal certificates, social security cards, and immigration paperwork.

All licenses contain machine-readable technologies (bar codes, magnetic strips) to provide the encoded details of the driver's license information, if a citation is issued in the field. A typical traffic stop in a jurisdiction using this technology can go something like this: The driver's license with a bar code or in some cases a magnetic stripe also, can be read by an in-car unit. This unit then transmits the information to the department's central computer that runs a standard check of traffic and criminal records on the individual. This information is returned to the car, either by the dispatcher or through an in-car computer. This same computer may display the photo of the driver from the driver's license database. Information on the type of violation is then entered into the unit. This generates the printed citation to be given to the driver and at the same time updates the departmental computer and transfers the violation information electronically to the courts and the DMV. Multiple entries of the same information or data entry errors are avoided, thus saving precious patrol time while.

All U.S. and Canadian jurisdictions have now deployed this technology. Work is progressing on standards (common data elements and compatible records) so that a national and, perhaps, an international network can be established. This progress emphasizes the importance of the law enforcement role to maintain a proactive relationship with motor vehicle departments.

In an effort to strike a reasonable balance between these competing interests and still address an escalating problem of fictitious, fraudulently altered and fraudulently obtained driver's licenses, the American Association of Motor Vehicle Administrators (AAMVA) invited the IACP, other law enforcement groups and vital statistics agencies to join a task force to work on ways to provide at least minimal standardization from jurisdiction to jurisdiction, and to combat fraud. One of the most controversial issues that the task force encountered is how to handle the problem of licenses for undocumented immigrants, and whether such licenses should be issued to expire when the individual's privilege to remain in the country expires.

Graduated Driver's Licenses (GDL)

Graduated Driver Licensing programs were designed to help reduce crashes amongst novice drivers by incorporating restrictions and minimizing their exposure to hazardous situations. The objective of a GDL program is to minimize motor vehicle crashes due to inexperience, high risk taking behavior, and high risk exposure by reducing and limiting hazardous exposures. By reducing hazardous exposures, it allows new drivers to safely gain driving experience before obtaining full driving privileges.

Three phases of a GDL Program:

- Learner Permit Phase
- Intermediate or Provisional Phase
- Full/Unrestricted Licensure

Currently there are no standardized national requirements for GDL programs. It is important to note that each State may have varying requirements and restrictions for each phase.

National Driver's License Compact

The Driver License Compact (DLC) was a major step necessary in helping to maximize law enforcement efforts against drunk drivers and other serious traffic offenders. The DLC was created to provide uniformity among the member jurisdictions when exchanging information with other members on convictions, records, licenses, withdrawals and other data pertinent to the licensing

process. The concept behind the DLC agreement was that each driver have only one driver license and one driver control record (DCR).

The Non Resident Violator Compact (NRVC) was developed to help standardize methods utilized by the various jurisdictions to process non-resident violators receiving citations, and their failure to appear or otherwise failure to comply with outstanding moving traffic summons. The NRVC allows participating jurisdictions to inform each other's motor vehicle administrations when a resident of one jurisdiction did not comply with the citation's term. Once the home jurisdiction motor vehicle administrator receives notice of a resident's citation noncompliance, the procedure for license suspension is initiated.

AAMVA supports the DLC / NRVC activities by providing Secretariat services and having an AAMVA Board Advisor in attendance at Compact Executive Board meetings.

For example, a driver charged with DUI in a Compact state will have his or her license suspended in his or her home state as well. Also, a nonresident driver can promise to appear in court, or to pay a waiver and be released without bond. If they fail to satisfy the court appearance, a mechanism permits the issuing state to revoke the driver's privileges until they comply with the laws of the other state.

Administrative License Revocation (ALR)

State government traditionally has retained the responsibility of issuing and regulating driver's licenses. Upon conviction, the courts have been permitted to limit or suspend driver's licenses or operating privileges. A current trend is to remove the license sanction from the courts, to eliminate unnecessary delays associated with court backlogs, and to reduce the impact of plea bargaining.

The National Highway Traffic Safety Administration advocates the on-the-spot revocation by police officers of the driver's licenses of those persons they arrest for driving under the influence of alcohol or drugs.

In states with this legislation, police officers are empowered to confiscate the driver's license of a person arrested for impaired driving when that person either refuses a chemical test of blood, breath or urine or tests above the prescribed limit. The license is usually forwarded to the licensing agency, and the holder is issued a temporary permit to drive pending a hearing. The benefit of ALR is that action is less complicated and immediately removes a known hazardous driver from the roads.

Most states have some version of ALR in operation; it is a condition for some states to receive additional federal highway safety funds. Although the system is claimed to get drunk drivers off the road more quickly, it is not without its critics. In some jurisdictions, the police feel that administrative law judges and hearing examiners are more prone to dismiss cases for hyper-technical reasons than are criminal court judges, and that the system just adds one more layer of complexity and ties police officers up at another hearing.

Detecting Suspended and Revoked Driver's Licenses

The revocation or suspension of a driver's license is potentially very effective because it prevents persons with physical or mental disabilities, as well as those with poor driving records or attitudes, from the other users of our highways.

In 2013, AAMVA published their Best Practices to Reducing Suspended Drivers. This publication includes research that reveals that approximately 40 percent of drivers suspended are suspended for non-driving reasons. Research further indicates that persons suspended for a driving reason are three times more likely to be involved in a crash than a person suspended for a non-driving reason. As a result, AAMVA recommends jurisdictions repeal laws and regulations requiring suspension for non-driving reasons. Implementation would result in 40 percent fewer suspended drivers and a commensurate reduction in resource drain on law enforcement and the courts. Moreover, the remaining suspended drivers would be the ones law enforcement should truly focus on removing from the roads. [1]

In practice, however, this strategy is not as effective as it should be, because many persons continue to drive after their driving privileges have been suspended or revoked and are not detected by law enforcement. This problem leads to a breakdown in respect for the law, places dangerous drivers on the roadways, and frustrates the criminal justice and driver's licensing processes.

Although detecting and apprehending suspended or revoked drivers is difficult, few police activities yield higher dividends in improving traffic safety and promoting respect for the law.

Repeated studies indicate that license suspensions are an effective sanction used in traffic law enforcement. For this reason, law enforcement generally opposes limited or "drive-to-work" licenses as a dilution of the law and too subject to potential abuse.

The Need for a Policy

Police agencies need policies to ensure that appropriate enforcement action is taken when a suspended or revoked driver's license is found. The policy should not permit an officer to lodge a charge of driving without a license as a substitute for driving after suspension. Policies should advocate that driving after suspension cases are pursued to conviction and not dropped as part of a plea bargain, especially when accompanied by DUI charges. When a

motorist displays a suspended or revoked license, the individual should be charged with that separate offense, as well as with driving after suspension. The license should be confiscated and returned to the state or provincial licensing agency.

Police agencies should form task forces to contact anyone who fails to turn in his or her driver's license, if it is under suspension or revocation. Officers should confiscate the license and return it to the licensing authority. The individual should be charged with failing to surrender a suspended or revoked license.

Violator-directed patrols are effective when police departments are notified by licensing agencies of the suspension or revocation of the driver's license of a person who is a habitual motor vehicle offender.

The National Driver Register (NDR)

The National Driver Register (NDR) is a central repository of information on individuals whose driver's licenses have been revoked, suspended, cancelled, or denied, or who have been convicted of certain serious traffic-related violations, such as driving while impaired by alcohol or other drugs.

When an individual applies for a license, state driver licensing officials query the NDR to determine if the individual's driving privilege has been withdrawn in any other state. Because the NDR is a nationwide index to driver records from all states, a state needs to submit only a single inquiry to obtain this information. The information obtained from the NDR assists state driver licensing officials in determining whether or not to issue a license.

The Federal Aviation Administration and the Federal Railroad Administration also use the NDR to process their inquiries for the detection of driving violations, especially alcohol-related ones, among their applicants for certification. In addition, the U.S. Coast Guard recently was authorized to receive NDR information regarding their applicants for certification.

Every state in the U.S. has established electronic access to the NDR file—a major step for states that issue licenses over the counter rather than require a waiting period.

As required by Public Law 97-364, the NDR has converted to a Problem Driver Pointer System (PDPS) to improve the timeliness and reliability of NDR information. Under the PDPS, the NDR no longer contains substantive data. Instead, it contains only identifying information to enable it to check whether or not adverse action has been taken against an individual—not specific information about *why* an individual's name appears in the NDR file; such information will be maintained by the state that executed the adverse action.

When a match occurs with a record on the NDR file, the NDR electronically points to the state where the adverse action is maintained, retrieves that information, and relays it to the state of inquiry. In this way, the state of inquiry is assured of receiving the latest information available regarding the driver's record.

Motorcycle Licensing Requirements

Motorcyclist deaths had been declining since the early 1980s but began to increase in 1998 and continued to increase through 2008. Motorcycle deaths accounted for 13 percent of all motor vehicle crash deaths in 2015 and were more than double the number of motorcyclist deaths in 1997. In 2015, motorcycle crashes were up 8.3 percent from 2014, according to the NHTSA. Forty-one percent of motorcyclist deaths in 2015 occurred in single-vehicle crashes, and 59 percent occurred in multiple-vehicle crashes. This has remained largely unchanged since the 1980s. [2]

To receive the proper endorsement in most states, individuals need to pass a knowledge and skills test by either a state licensing agency or state sponsored rider education course.

The Problem of Unlicensed Motorcyclists

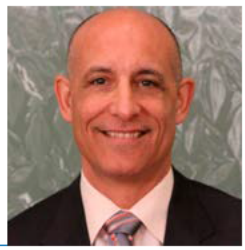
Despite many states having licensing requirements, motorcyclists continue to operate without a valid license. In 2015, 27 percent of fatally injured motorcycle drivers were operating without a valid motorcycle license at the time of the collisions, while only 13 percent of passenger vehicle drivers in fatal crashes did not have valid licenses. Motorcycle riders involved in fatal crashes were 1.3 times more likely than passenger car drives to have previous license suspensions or revocations. [3]

Notes:

1. "Best Practices Guide to Reducing Suspended Drivers," *American Association of Motor Vehicle Administrators,* 2013, www.aamva.org/workarea/downloadasset.aspx?id=3723
2. "Traffic Safety Facts," *National Highway Traffic Safety Administration*, 2017, https://crashstats.nhtsa.dot.gov/Api/Public/Publication/812353
3. National Center for Statistics and Analysis. (2017, March). Motorcycles: 2015 data (Updated, Traffic Safety Facts. Report No. DOT HS 812 353). Washington, DC: National Highway Traffic Safety Administration

CHAPTER 7: REGISTRATION, TITLE AND INSPECTION ENFORCEMENT

Registration, Title and Inspection Enforcement



By: **Brian Ursino,** *Director of Law Enforcement,* American Association of Motor Vehicle Administrators (AAMVA)

License plates serve one common purpose across the states and provinces throughout North American jurisdictions; to identify motor vehicles. They also identify vehicle registrants and demonstrate compliance with motor vehicle registration laws.

License Plate Design and Manufacture

License plates are most effective when they are designed to optimize legibility to the human eye as well as for automated license plate readers (ALPR). The ability for law enforcement and citizens to quickly and easily identify license plate numbers (consisting of alpha and/or numeric characters) is fundamental to accurate vehicle identification.

Toward that end, law enforcement has a vested interest in ensuring the plates issued by their state comply with the License Plate Standard published by the American Association of Motor Vehicle Administrators in August 2016. The adoption of the administrative, design and manufacturing recommendations contained in this standard are intended to streamline the license plate retrieval processes within motor vehicle agencies, support highway safety, and increase certain revenue collection which is dependent on accurate license plate identification, such as toll collection, restricted lane access and parking regulations. License plate recognition, by human eye and ALPR, is critical to serving these purposes.

In addition, license plates play a central role in preventing and solving crimes. Every day across North America, crimes are prevented or solved through the identification of a license plate. It is difficult to quantify the missed opportunities that occur to prevent or solve a crime because a license plate was misread by either the human eye, or by ALPR, but testing has documented that misreads occur. Adoption of the license plate standards contained in this document will minimize the risk of such misreads.

Two-Plate Reflectorized Registration

Mandating that all vehicles display registration plates on both the front and rear of the vehicle enhances law enforcement's efforts to identify a vehicle rapidly, whether it is from a frontal position or from the rear of the vehicle. Police officers are commonly trained to jot down the license plate numbers of oncoming vehicles they see while responding to a collision or crime scene, in an effort to identify possible fleeing perpetrators or eyewitnesses to the incident. Bicyclists, pedestrians and drivers frequently observe the plate numbers of suspicious vehicles and report them to the police. This assistance has been instrumental in solving many serious crimes over the years.

To read more on the support of the AAMVA and the IACP policy position on license plates, please refer to the AAMVA and the IACP websites.

If for no reason other than officer and public safety, two-plate reflectorized registration should be incorporated as a primary design for registration plates in every jurisdiction. Additionally, a reflectorized plate aids in the prevention of collisions with vehicles parked along streets in poorly lighted areas.

The proliferation of different plate types bearing the same characters creates problems in proper vehicle identification and states should avoid issuing duplicate plate numbers.

Enforcing the Two-Plate Requirement

Vehicles required by law to display two registration plates are easier to identify, and the dual plate registration is effective in thwarting vehicle thefts.

In those jurisdictions where two plates are required, the absence of one plate provides an officer with articulable, reasonable suspicion to execute a traffic stop for a vehicle registration inquiry, leading to the detection of impaired drivers, persons operating under revocation or suspension, and persons transporting contraband.

It should be the responsibility of law enforcement and other public agencies to demonstrate and convey both to the public and to legislative bodies the benefits derived from a two-plate system. Vehicle owners can see potential benefits in the event their vehicles are stolen. Citizens can appreciate how the two-plate system enhances police officers' abilities to detect criminals and simultaneously heightens personal safety.

Police executives and associations should be proactive in advocating two-plate systems in jurisdictions that do not have them and in fighting back attempts to go to a one-plate concept. However, justifying the need for a two-plate system is difficult unless law enforcement officers aggressively enforce the two-plate requirement by stopping vehicles with only one plate and issuing either warnings or

citations to these drivers. Each police department should have a specific policy supporting enforcement against drivers with missing, mutilated, or illegible number plates.

Title Enforcement

Within the law enforcement community, title enforcement responsibilities usually do not generate discussion; however, without specialized training and concentration in vehicle titling and registration, the public can suffer astronomical fraud and economic loss.

Title enforcement requires investigating law enforcement personnel to have a comprehensive knowledge of federal, state and local laws, regulations, and ordinances and to understand the lack of uniformity between the various types of titles, duplicate titles, salvage titles, and manufacturer's statements of origin. As with most sophisticated law enforcement areas and functions, specialty skills have evolved that are essential to effectiveness.

The National Motor Vehicle Title Information System (NMVTIS) is a database operated by AAMVA. NMVTIS tracks vehicle history from cradle to grave and is designed to protect consumers from fraud and unsafe vehicles as well as keeping stolen vehicles from being re-sold. NMVTIS also has a "Law Enforcement Access Tool" specifically designed to assist law enforcement in deterring and detecting title fraud and other vehicle related crimes.

Hidden VIN

Beginning in 1981, all motor vehicles manufactured in the United States or imported for sale for on-road use were required to have 17-character vehicle identification numbers (VINs). With the enactment of the Federal Motor Vehicle Theft Law Enforcement Act of 1984, vehicles with high-theft potential were further required to use component part labeling. This secondary source of identification, the so-called "hidden VIN" (frame stamping, firewall stamping, transmission cross-members, engine markings, and transmission markings), may be used by specially trained officers to verify the authenticity of vehicles and/or of component parts. This secondary source of identification is required by law to be indelibly printed on a label or "inscribed" directly into a vehicle part. This label must be permanently affixed to the component part on an interior surface or location, so it cannot be damaged in a collision or during part installation, adjustment, or removal. It must be located in such a fashion as to prevent its destruction or defacement during normal dealer preparation, including any after-market installation procedures. The label must contain the manufacturer's logo, or some other unique identifier, plus the VIN. Any attempt to alter the label must either leave traces of the original number or visibly alter the label's appearance. In cases of non-label identifiers, inscriptions to the part must be so that any removal or alteration visibly changes the appearance of the vehicle part.

The location of secondary sources of identification is made at the discretion of the vehicle manufacturer. Manufacturers must notify the National Highway Traffic Safety Administration (NHTSA) in writing of their number system and their locations within 308 days of the date the vehicle line is offered for sale.

Having the special expertise to utilize secondary sources of vehicle identification to investigate cases is invaluable to a police agency. The National Insurance Crime Bureau (NICB), a private organization funded by the automobile manufacturers and insurers, has special agents available to assist law enforcement agencies on a regional basis to provide training and other technical assistance in identifying hidden VINs.

Periodic Motor Vehicle Inspection

Approximately, 17 U.S. states, plus several U.S. territories and Canadian provinces, have some type of a periodic motor vehicle inspection (PMVI) program for passenger vehicles. These jurisdictions require annual or semi- annual safety inspections at either state-maintained or private motor vehicle inspection stations licensed by jurisdictional authorities. For commercial vehicles and school buses, many jurisdictions require more frequent inspections. Law enforcement agencies are often charged with using specially trained officers or inspectors to perform additional inspections of school buses.

In other jurisdictions, periodic safety inspections by an authorized inspection station are not required, but officers are allowed to stop vehicles to conduct roadside safety inspections.

Although variation exists within the types of PMVI programs, most ensure the periodic inspection of basic safety components, such as steering, tires, suspension, brakes, lighting systems, and glass.

In addition, increased concern by the Environmental Protection Agency (EPA) over air pollution caused by vehicle emissions has led many jurisdictions to require periodic testing of motor vehicle emission systems. This procedure can be effectively combined with periodic safety inspections in a single system. Because PMVI programs help ensure the integrity of basic motor vehicle safety systems, law enforcement executives and associations are encouraged to lobby for enacting PMVI in those states and provinces where it does not currently exist.

Effectiveness of PMVI Programs

Studies conducted by the National Highway Traffic Safety Administration (NHTSA) have identified vehicle defects as

the sole cause in a significant number of fatal crashes. In addition, it has been determined that vehicle defects play a partial role in a much larger percentage of all collisions. The failure of essential mechanical vehicle components—such as ball joints, idler arms, rack and pinion steering units, shock absorbers or struts, tires, and brakes—can cause loss of control of a motor vehicle while it is in motion.

Public Support for PMVI

While PMVI programs are not always recognized for the benefits they deliver, public support does exist for such programs. Public perception in some regions is that the benefits derived from the inspection outweigh the inconvenience or cost of having to take a vehicle to a service facility for an inspection. Without a PMVI program, what would be a simple, low-cost replacement of brake pads often leads to the expensive replacement of rotors simply because the problem was not caught in time. Thus, PMVI programs can actually reduce the cost of motor vehicle maintenance, as well as enhance safety factors.

Law Enforcement Benefits and Concerns

With the conscientious efforts of state agencies, street-level enforcement officers, and public advocacy groups, a PMVI program can be effectively administered and enforced and can contribute enormously to highway safety. Requiring an inspection sticker on a vehicle also gives the police additional articulable, reasonable suspicion to stop a vehicle, and frequently leads to the detection of drunken drivers, revoked or suspended operators, persons transporting contraband, or stolen vehicles. Although not the primary purpose of a PMVI program, this enforcement tool can provide significant additional public safety benefits.

Rebuilt Vehicles

Motor vehicle thieves often utilize rebuilt or reassembled vehicles to conceal the identities of stolen vehicles. Using parts salvaged from several stolen vehicles to rebuild another vehicle, the thief then represents the stolen vehicle as one rebuilt and thereby is able to secure the proper documentation to legitimize the sale of the vehicle. Secondary concerns regarding rebuilt vehicles are the level of safety those vehicles provide to their occupants and their roadworthiness. Law enforcement officials must take specific measures to ensure that stolen vehicles are not legitimately sold in the public market, and that unsafe vehicles are not allowed to operate on the highways. Rebuilt vehicles can offer an affordable alternative to individuals who otherwise could not purchase vehicles, but unscrupulous or incompetent rebuilders may shortcut or overlook critical safety components. For this reason, all rebuilt vehicles should be inspected for safety compliance. A check of all vehicle safety equipment should be performed to assure compliance with applicable statutory requirements.

To prevent the sale of stolen vehicles, law enforcement personnel should examine all salvaged or rebuilt vehicles prior to issuing titles. Specially trained VIN examiners, generally at the state level, should closely scrutinize each such vehicle for signs of repair and/or part replacement. The examination should include a review of documentation to ensure all replacement parts are accounted for and that component part labels or inscriptions are intact and free of tampering. Any discrepancy should be thoroughly investigated, including an examination of major component part labels and identifiers

Specially Constructed Vehicles

Specially constructed vehicles, "street rods," and other assembled vehicles pose many of the same problems as rebuilt vehicles. A specially constructed vehicle generally is not visually recognizable as being produced by a particular manufacturer, while an assembled vehicle is distinguishable because its composition is by a well-known manufacturer of commercially produced vehicles.

When the owner of a specially constructed or assembled vehicle requests a title or registration, law enforcement and vehicle titling authorities should ensure that the vehicle is examined for safety compliance. Such vehicles should be required to meet and be in compliance with all state equipment laws prior to final inspection and the issuance of a title.

A particular problem involves vehicles fitted with oversize tires or "jacked up" by other means so that they are extremely high on the road and their centers of gravity have been drastically altered. Such alterations can impair the handling dynamics of such vehicles and lead to component failure and dangerous traffic crashes.

When such vehicles slip through the registration process, street-level law enforcement officers are obligated to enforce state laws and local ordinances regarding such standards as bumper height requirements. Law enforcement agencies should have written policies encouraging their officers to enforce these requirements.

AAMVA has developed two best practice guides that may be useful:

Best Practices for the Title and Registration of Rebuilt and Specially Constructed Vehicles (2012)

http://www.aamva.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=4748&libID=4725

Best Practices for Title and Registration of Reconstructed and Replica Vehicles (2013)

http://www.aamva.org/WorkArea/DownloadAsset.aspx?id=4752

CHAPTER 8: UNIFORMITY, RECIPROCITY AND FEDERAL PROGRAMS

Federal Agencies and Grants

The following is a summary of the various federal agencies that are active in highway safety and traffic enforcement, along with their roles and responsibilities.

The U.S. Department of Transportation National Highway Traffic Safety Administration (NHTSA)

Website: https://www.nhtsa.gov/about-nhtsa

The National Highway Traffic Safety Administration (NHTSA) was established by the Highway Safety Act of 1970, as the successor to the National Highway Safety Bureau, to carry out safety programs under the National Traffic and Motor Vehicle Safety Act of 1966 and the Highway Safety Act of 1966. It also administers consumer programs established by the Motor Vehicle Information and Cost Savings Act, enacted in 1972.

NHTSA's mission is to save lives, prevent injuries and reduce economic costs due to road traffic crashes, through education, research, safety standards and enforcement activity.

NHTSA also sets safety standards for motor vehicles and associated equipment, investigates possible safety defects, assures that products meet safety standards and are not defective (through recalls if necessary) and tracks safety-related recalls. The agency also enforces regulations on fuel economy, odometer fraud, and vehicle theft.

402 Funds

The State Highway Safety Program, commonly referred to as Section 402, was initially authorized by the Highway Safety Act of 1966 and has been reauthorized and amended a number of times, including most recently on December 4, 2015, when the President signed into law the Fixing America's Surface Transportation Act (FAST Act), Public Law 114–94.

Section 402 funds are used to support countermeasure strategies and projects identified in the States' Highway Safety Plan (HSP). This includes resources to initiate new projects and catalyze or accelerate existing projects to address major safety issues with well-planned strategies, and leverage additional State and local investment in highway safety. States must have an approved HSP to receive Section 402 grant funds. To review eligibility determination, qualification criteria, and use of grant funds, reference: 23 CFR Part 1200.

The program is administered by the National Highway Traffic Safety Administration (NHTSA) at the Federal level and by the State Highway Safety Offices (SHSO) at the State level.

Under the FAST Act, states are required to have a highway safety program that is approved by the Secretary. Funds can be spent in accordance with national guidelines for programs to:

- Reduce drug- and alcohol-impaired driving
- Reduce speeding
- Encourage the use of occupant protection
- Improve motorcycle safety
- Improve pedestrian and bicycle safety
- Reduce school bus deaths and injuries
- Reduce crashes from unsafe driving behavior
- Improve enforcement of traffic safety laws
- Improve driver performance
- Improve traffic records
- Enhance emergency services
- Increase awareness of commercial motor vehicles
- Support school-based driver's education classes

In addition, states may (but are not required to) spend 402 funds on teen driver programs. If they do choose to fund these programs, they must fund only strategies authorized under 23 USC 402(m). No 402 funds can be spent on the implementation of automated enforcement programs.

States must submit an annual Highway Safety Plan (HSP) which must be data-driven and set quantifiable, annual performance targets for 15 performance measures. The plan must include strategies that will allow the state to meet its performance targets and must describe its successes in meeting its performance targets in the previous fiscal year.

States are required to submit their Section 402 and Section 405 consolidated grant application by July 1 of each fiscal year. The National Highway Traffic Safety Administration (NHTSA) will have 60 days (45 days beginning with FY 2018) to review and approve or disapprove the consolidated grant application.

Funds are apportioned to the states under the same formula as MAP-21: 75 percent population and 25 percent road-miles. At least 40 percent of Section 402 funds must be spent by local governments or be used for the benefit of local governments.

For exact dollar amounts, funding charts by fiscal year can be found on the Federal Grant Programs page under «Highway Safety Funding.»

Section 402 of title 23 of the United States Code requires the Secretary of Transportation to promulgate uniform guidelines for State highway safety programs. These guidelines offer direction to States in formulating their highway safety plans for highway safety efforts that are supported with section 402 and other grant funds. The guidelines provide a framework for developing a balanced highway safety program and serve as a tool with which States can assess the effectiveness of their own programs. NHTSA encourages States to use these guidelines and build upon them to optimize the effectiveness of highway safety programs conducted at the State and local levels. The Guidelines may be found at: https://one.nhtsa.gov/nhtsa/whatsup/tea21/tea21programs/index.htm.

Section 403

Section 403 funds demonstration grants (in addition to other programs) to develop new approaches and strategies to reduce motor-vehicle-related deaths and injuries.

Section 404: High-visibility enforcement program comprises not less than 3 campaigns in each of fiscal years 2016 through 2020. The purpose of each campaign carried out shall be to achieve outcomes related to not less than one of the following objectives:

1. Reduce alcohol-impaired or drug-impaired operation of motor vehicles.
2. Increase use of seatbelts by occupants of motor vehicles.

Incentive Funds

NHTSA FY2019 Section 405 Grant Determinations Table

NHTSA Highway Safety Grants Resources Guide

Section 405: Under the FAST Act, Section 405 is the National Priority Safety Program, which provides grant funding to address selected national priorities for reducing highway deaths and injuries. Previously authorized under MAP-21, the FAST Act made no substantive changes to many of the grants (Occupant Protection, State Traffic Safety Improvements, Impaired Driving Countermeasures and Motorcyclist Safety). Limited changes were made to the Alcohol-Ignition Interlock Law, Distracted Driving and Graduated Driver Licensing Incentive grants. The FAST Act added two new grants, 24-7 Sobriety Program and Nonmotorized Safety.

All are administered by the National Highway Traffic Safety Administration (NHTSA) at the federal level and the State Highway Safety Offices (SHSOs) at the state level.

Each program is authorized as a separate section or tier within Section 405, and each has its own eligibility criteria. States must satisfy the eligibility criteria of each tier in order to receive funding for that tier. States must submit their Section 405 applications on July 1 as part of the consolidated application process.

For exact dollar amounts, funding charts by fiscal year can be found on the Federal Grant Programs page under «Highway Safety Funding.»

Section 405(d): Impaired Driving Countermeasures

- 52.5 percent of Section 405 funds are earmarked for impaired driving incentive grants to reduce the risk of driving under the influence of alcohol, drugs or a combination of the two. There is a maintenance of effort requirement and states would have to provide a 20 percent matching share. All states receive funds under this tier. They are divided into low-, medium-, and high-range states based on the most recent three years of FARS data. Low-range states do not have to satisfy specific eligibility requirements. The requirements increase for the other two types of states. Low-range states have more flexibility in the use of funds than medium- or high-range states and may use up to 50 percent of the funds for any Section 402 purpose, in addition to qualifying by having an interlock program.
- States with a compliant 24-7 sobriety program also qualify for funding .The State must have a law the requires all individuals convicted of driving while intoxicated to receive restricted driving privileges for at least 30 days, and, must have a law or program that authorizes a statewide 24-7 sobriety program.
- 12 percent of this tier is earmarked for ignition interlock incentive funds. States that have an all-offender ignition interlock law, with certain limited exceptions allowed by the FAST Act, will be eligible for these grants. Eligible states can use these funds for any purpose under 402. States qualifying with a 24-7 program receive 3 percent of available funding States can qualify with both provisions and receive a total of 15 percent of available funding.

Section 405(e): Distracted Driving

8.5 percent of Section 405 funds are earmarked for distracted driving incentive grants. The FAST Act amended the qualifications, revising the Comprehensive Distracted Driving grant to provide more flexibility and establishing a new Special Distracted Driving grant for two fiscal years for States that do not qualify for the Comprehensive grant. States must enact and enforce a prohibition on texting as well as a ban of the use of all electronic devices for all drivers aged 18 and younger, plus additional requirements. Eligible states can use 50 percent of the funds for Section 402 purposes and 50 percent for distracted driving purposes. The FAST Act allows states with distracted driving data that conforms to the most recent MMUCC to use 75 percent of the funds for Section 402 purposes. $5 million of these funds are earmarked for a national media campaign on distracted driving.

Section 405(f): Motorcyclist Safety - Section 405(g): State Graduated Driver Licensing Laws

5 percent of Section 405 funds are earmarked for graduated driver licensing (GDL) incentive grants. States have to require a two-stage driver license and satisfy specific criteria for the learner's and intermediate stages. The FAST Act changed the age requirement to 18 (rather than younger than 21) and some other requirements are less prescriptive. Eligible states can use 25 percent of the funds for GDL-related purposes and 75 percent for any purpose under Section 402. If a state is in the lowest 25 percent of states for under-18 age drivers involved in fatal crashes per the total number of under-18 drivers in the state, the state may use 100 percent of the funds for any Section 402 purpose.

Section 405(h): Non-motorized Safety

5 percent of Section 405 funds are earmarked for non-motorized safety incentive grants. States would have to provide a 20 percent matching share, the only incentive grant with a specified federal fund limit. States are eligible if the annual combined pedestrian and bicyclist fatalities in the state exceed 15 percent of the total annual crash fatalities in the State using the most recently available final data from NHTSA's FARS. Eligible states may use grant funds *only* for training law enforcement on state laws applicable to pedestrian and bicycle safety; enforcement mobilizations and campaigns designed to enforce those state laws, or, public education and awareness programs designed to inform motorists, pedestrians and bicyclists of those state laws.

Section 1906: Racial Prohibition Grants

The Section 1906 Racial Prohibition Grants program was authorized under SAFETEA-LU. It was administered by NHTSA at the federal level and the State Highway Safety Offices (SHSOs) at the state level. Although this program was *not* reauthorized under MAP-21, the FAST Act revived the grant program for FY 2017-2020 with some changes and the law requirement was removed.

This program provides grants to encourage states to maintain and allow public inspection of statistical information on the race and ethnicity of the driver for all motor vehicle stops made on all public roads except local or minor rural roads.

Under the FAST Act, a state is eligible for a grant by:

1. Maintaining and allowing public inspection of statistical information on the race and ethnicity of the driver for each motor vehicle stop made by a law enforcement officer of a Federal ad highway or,
2. Undertaking activities during the fiscal year of the grant to do so.

Eligible states are able to use grant funds to:

1. Collect and maintain data on traffic stops; or,
2. Evaluate the results of the data

The FAST Act authorizes the Section 1906 program at $7.5 million each year for FY2017 – 2020. Eligible states cannot receive more than 5 percent of the total annual funding. A state may not qualify by providing assurances for grants for more than two years. The federal share payable is 80 percent. States may use grant funds only for the costs of:

1. Collecting and maintaining data on traffic stops, and
2. Evaluating the results of the data. Funds remaining available each fiscal year may be reallocated by NHTSA to carry our activities authorized under Section 403.

For Additional Resources: http://www.ghsa.org/about/federal-grant-programs/405 & http://www.ghsa.org/about/federal-grant-programs/1906

The Federal Highway Administration

Website: https://www.fhwa.dot.gov/

The Federal Highway Administration (FHWA) was established as a component of the Department of Transportation in 1967 as a result of the Department of Transportation Act (49 U.S.C. app. 1651 note). The FHWA supports State and local governments in the design, construction, and maintenance of the Nation's highway system (Federal Aid Highway Program) and various federally and tribal owned lands (Federal Lands Highway Program). Through financial and technical assistance to State and local governments, the Federal Highway

Administration is responsible for ensuring that America's roads and highways continue to be among the safest and most technologically sound in the world.

Federal-Aid Highway Program

The FHWA administers the Federal-aid highway program of financial assistance to the states for highway construction and improvements. This program provides for construction and preservation of the National System of Interstate and Defense Highways, financed generally on a 90-percent Federal, 10-percent state basis, and the improvement of other Federal-aid roads, with financing generally on an 80-percent Federal to 20-percent state basis.

The agency also administers the Highway Bridge Replacement and Rehabilitation Program to assist in the inspection, analysis, and rehabilitation or replacement of bridges both on and off the federal-aid highway systems.

The FHWA is responsible for carrying out several highway safety programs. These safety programs provide funding for projects which remove, relocate, or shield roadside obstacles; identify and correct hazardous locations; eliminate or reduce hazards at railroad crossings; and improve signing, pavement markings, and signalization.

The agency promulgates and administers highway-related safety guidelines providing for the identification and surveillance of crash locations; highway design, construction, and maintenance; traffic engineering services; and highway-related aspects of pedestrian safety.

Federal Motor Carrier Safety Administration

Website: https://www.fmcsa.dot.gov/

The Federal Motor Carrier Safety Administration (FMCSA) is the lead Federal government agency responsible for regulating and providing safety oversight of commercial motor vehicles (CMVs). FMCSA's mission is to reduce crashes, injuries and fatalities involving large trucks and buses.

FMCSA exercises federal regulatory jurisdiction over the safety performance of all commercial motor carriers (trucks and buses) engaged in inter- state and foreign commerce. The agency's motor carrier safety investigators conduct safety reviews at the carriers' facilities and at roadside to determine the safety performance of the carriers' operations. Compliance reviews are conducted to follow up on problem areas identified during the safety reviews and at times result in prosecution or other sanctions against violators of the federal motor carrier safety regulations or the hazardous materials transportation regulations.

Grant Funds

The FMCSA safety grant funding opportunities are primarily available to State and local government agencies in one of the 50 States, the District of Columbia, Puerto Rico, Northern Mariana Islands, American Samoa, Guam, and the US Virgin Islands. Applicants for FMCSA funding opportunities should be working on commercial motor vehicle safety activities and should demonstrate a capacity to work with highway traffic safety stakeholders which may include, but are not limited to, State and local law enforcement agencies, State departments of public safety, departments of transportation, State traffic records coordinating committees, associations that focus on commercial motor vehicle safety and training issues, and other industry stakeholders.

Commercial Driver's License (CDL) Program

The Commercial Driver's License (CDL) Program Implementation Grant provides financial assistance to States to achieve compliance with the requirements of 49 CFR Parts 383 and 384. Additionally, the CDLPI grant program provides financial assistance for other entities capable of executing national projects that aid States in their compliance efforts and that will improve the national Commercial Driver's License (CDL) program.

The goal of the national CDL program is to reduce the number and severity of commercial motor vehicle crashes in the United States by ensuring that only qualified drivers are eligible to receive and retain a CDL.

Federal Law Enforcement Training Center

Website: https://www.fletc.gov/

The Federal Law Enforcement Training Center (FLETC), a bureau of the U.S. Department of Homeland Security FLETC serves a leadership role as the U.S. Federal Government's principal provider of world class, interagency training of Federal law enforcement personnel. The FLETC prepares new and experienced law enforcement professionals to fulfill their responsibilities in a safe manner and at the highest level of proficiency. Training consists of all phases of law enforcement instruction, from firearms and high-speed vehicle operations, to legal case instructions and defendant interview techniques. The FLETC delivers interagency training with optimal efficiency through the government-wide sharing of facilities, equipment and expertise which produces economies of scale available only from a consolidated law enforcement training organization.

It is through consolidated training that the FLETC can respond quickly to emerging training needs, readily adapt

to new requirements and focus exclusively on training, which is FLETC's only mission. The FLETC currently provides law enforcement training to over 80 Partner Organizations. The FLETC also trains state, local, tribal, campus, and international law enforcement officers and agents. The number of agencies attending training, the number of students trained and the number of student-weeks delivered have steadily increased over the FLETC's 37-year history.

NHSTA Regional Offices

Regional Administrator NHTSA – Region Office 1
Volpe National Transportation Systems Center,
55 Broadway
Kendall Square—Code 8E
Cambridge, MA 02142
(617) 494-3427
Email: Region1@dot.gov

Regional Administrator NHTSA – Region Office 2
245 Main Street, Suite 210
White Plains, NY 10601
(914) 682-6162
Email: Region2@dot.gov

Regional Administrator NHTSA – Region Office 3
31 Hopkins Plaza, Room 902
Baltimore, MD 21201
(410) 962-0090
Email: Region3@dot.gov

Regional Administrator NHTSA – Region Office 4
Atlanta Federal Center
61 Forsyth Street, S.W.
Atlanta, GA 30303
(404) 562-3739
Email: Region4@dot.gov

Regional Administrator NHTSA – Region Office 5
4749 Lincoln Mall Drive, Suite 300B
Matteson, IL 60443
(708) 503-8822
Email: Region5@dot.gov

Regional Administrator NHTSA – Region Office 6
819 Taylor Street, Room 8A38
Fort Worth, TX 76102
(817) 978-3653
Email: Region6@dot.gov

Regional Administrator NHTSA – Region Office 7
901 Locust Street, Room 466
Kansas City, MO 64106
(816) 329-3900
Email: Region7@dot.gov

Regional Administrator NHTSA – Region Office 8
12300 West Dakota Avenue, Suite 140
Lakewood, CO 80228
(720) 963-3100
Email: Region8@dot.gov

Regional Administrator NHTSA – Region Office 9
John. E. Moss Federal Building
650 Capitol Mall, Suite 5-400
Sacramento, CA 95814
(916) 498-5058
Email: Region9@dot.gov

Regional Administrator NHTSA – Region Office 10
3140 Jackson Federal Building
915 Second Avenue
Seattle, WA 98174
(206) 220-7640
Email: Region10@dot.gov

FHWA Field Services/ Resource Centers

Eastern Field Services/Resource Center
Center 10 South Howard Street, Suite 4000
Baltimore, Maryland 21201-2819
(410) 962-0093

Midwestern Resource Center
One Prairie Office Center
4749 Lincoln Mall Drive, Suite 600
Matteson, Illinois 60461-1021
(708) 283-3500

Field Services
12300 West Dakota Avenue, Suite 340
Lakewood, Colorado 80228
(720) 963-3250

Southern Field Services/Resource
61 Forsyth Street, S.W., Suite 17T26
Atlanta, Georgia 30303
(404) 562-3570

Western Resource Center
201 Mission Street, Suite 1700
San Francisco, California 94105
(415) 744-3100

CHAPTER 9: EMERGING AND CRITICAL ISSUES IN TRAFFIC SAFETY

Traffic Safety's Critical Role in the Law Enforcement Mission

By: **William P. Georges,** *Assistant Chief (Ret.)*, Albany, New York, Police Department

Leadership is an important concept in law enforcement, and every member of an agency from the chief executive to field training officers should strive to both lead and provide guidance to personnel that results in long-term benefits for both the agency and the community it serves. There are numerous factors and changing situations that negatively impact every community, and, as a result, an agency's priorities are constantly shifting.

One of the factors that is omnipresent is traffic safety. Illegal and unsafe driving are problems that negatively impact every community. From crashes and the related problems that result from them to neighborhood complaints about speeding and other violations, traffic safety is a daily issue affecting law enforcement; as such, traffic safety should be a core component of every agency's overall mission.

While the first reaction to this statement may be "sure, we do traffic," often, traffic enforcement is sometimes viewed as a "have to do," but not a "need to do." Also, at times, traffic-related activities are decreased due to factors such as shifting priorities and assignments, increased calls for service, decreased personnel levels, and so forth. It is important to understand why maintaining or, in some cases, beginning or enhancing a comprehensive traffic safety program is important and how this activity can provide myriad benefits to a community and enhanced overall public safety.

First of all, as simple as this statement may sound, traffic enforcement is law enforcement! Every traffic stop is basically an investigation. Did the motorist knowingly commit the violation? Are there extenuating circumstances? Is the driver impaired and, if so, by what means? Are the occupants of the vehicle really who they say they are? Is there additional criminal activity beyond the initial reason for the stop? With a crash investigation, especially in a serious crash, an in-depth investigation must be conducted. What actions or factors contributed to the crash? Are there traffic violations and, if so, what are they? Is the driver impaired? Is the driver properly licensed? What other factors might have contributed to the crash? Investigators must interview witnesses, examine physical evidence, determine the minimum initial speed each vehicle was traveling, determine if there are possible vehicle defects, take measurements and photos, do scale drawings, and carry out other related investigative tasks. The skills required for these law enforcement duties are similar to any other investigation—and it's just as important that these investigations be taken seriously and be performed with diligence.

A comprehensive traffic safety plan can benefit a community and its residents in many ways, including reducing unsafe driving, contributing to investigations, and improving community-police relations. In order to capitalize on a traffic safety plan's full potential, it is necessary to examine the different areas that can be affected and the components that can be initiated by an agency.

Decreasing Crashes and Unsafe Driving

When one speaks of traffic safety, the mission of reducing crashes and unsafe driving is understandably what most people think of first—and with good reason. Most law enforcement personnel are familiar with crash data, but the numbers are worth mentioning. Every year, crashes kill or seriously injure people while also costing millions in medical, lost property, and other costs. In 2017, the National Highway Traffic Safety Administration (NHTSA) reported that 37,133 people were killed in traffic crashes in the United States. While efforts in enforcement, education, engineering, and EMS have slightly decreased this number in the past few years, the current death and injury rates on U.S. roadways are still alarming. This is not only a traffic safety problem, but also a public health problem. What do data show about the impact on your community? How can law enforcement improve this dangerous condition and better safeguard community members? The answer is clearly a comprehensive traffic safety program, and a variety of efforts and initiatives can be conducted by a single department or, as has been done in many jurisdictions, by multiple agencies working together in a single operation, thus expanding the area covered by the initiative and using collaboration as a force multiplier.

Crime and Traffic Safety

Effective and balanced traffic enforcement can often lead to the discovery of or leads for other criminal offenses. One need only look to general news sources to see cases where an initial traffic stop led to additional criminal investigations or arrests. From driving while impaired by alcohol or drugs, to the possession of narcotics or firearms, to human trafficking and wanted persons, traffic stops often are the foundation for other criminal arrests. With good investigative skills, traffic stops can often result in additional charges. As a result, increasing traffic enforcement does have the potential to also increase other types of criminal apprehensions.

It is also important to monitor, analyze, and understand the relationship between crime and traffic safety in a jurisdiction. Using the Data-Driven Approaches to Crime and Traffic Safety (DDACTS) model can greatly enhance an agency's analysis of both crash and crime activity and the nexus between them. This NHTSA program, developed in partnership with the IACP and several other organizations, provides the framework for analysis of timely and accurate data as they relate to both traffic enforcement and crashes and to crime and has proven very useful in effective analysis and personnel deployments. Additional information on DDACTS can be found on NHTSA's website at www.nhtsa.gov.

Traffic Enforcement as a Component of Community Policing

For many community members, a traffic stop may be the only contact that they will ever have with law enforcement, so educating people about the importance of traffic safety is a key factor in these encounters. Just issuing a citation negates an opportunity to positively interact with community members. It is important that they understand the dangers of unsafe driving and the heartache that it has the potential to cause them and others. Officers need to ensure that community members understand that traffic enforcement is not done for revenue generation and is conducted in locations where data show that dangers exist or when a violation is observed. Some agencies offer motorists a pamphlet explaining how or why traffic safety benefits their community. There are obviously several options that law enforcement personnel have when stopping a person for an offense. There is a citation, a warning ticket, or an oral warning, among other options, but the most important actions are terminating the offense and educating the offender. Having community members understand the importance of traffic safety and the positive impact that it can have on their quality of life through both enforcement and educational efforts, such as child safety seat checks, pedestrian and bicycle safety, impaired driving informational sessions, and other activities, can be an integral part of a community policing model.

Allied Organizations

There are numerous organizations, both public and private, that are available to assist an agency with its traffic safety mission. One of the most important is a state's Highway Safety Office (SHSO). Every law enforcement agency should maintain a good relationship with its SHSO and take advantage of its expertise and resources. In addition to NHTSA and SHSOs, the following allied organizations can assist agencies with a variety of matters, including data and analysis, programs, material, and subject matter expertise:

- American Association of Motor Vehicle Administrators (AAMVA)
- Federal Highway Administration (FHWA)
- Federal Motor Carrier Safety Administration (FMCSA)
- Federal Railroad Administration (FRA)
- Foundation for Advancing Alcohol Responsibility (FAAR)
- Governors Highway Safety Association (GHSA)
- Mothers Against Drunk Driving (MADD)
- National Safety Council (NSC)
- Safe Kids Worldwide

Additionally, IACP's Highway Safety Committee is a resource for IACP members. The committee comprises representatives from international, federal, state, county, and municipal agencies, along with representatives from allied organizations. The committee and its members are available to assist IACP members with traffic safety issues.

From a serious vehicle crash, to a resident's complaint of cars speeding through the neighborhood and endangering children, to other problems caused by traffic-related issues, law enforcement agencies are impacted by traffic safety on a daily basis. Main-taining a comprehensive traffic safety program consisting of data-driven enforcement, education, and engineering as a core component of an agency's mission will serve to enhance public safety, work as a part of community policing efforts, and ultimately produce positive benefits. Traffic safety should always be mission critical for both the agency and its personnel.

Traffic Enforcement: Back to the Basics

By: **Howard B. Hall,** *Chief of Police,* Roanoke County, Virginia, Police Department and **Anthony S. Lowman,** *Major,* Maryland State Police

Quite a few years ago, as the authors were completing selection processes and training academies, they were each asked repeatedly why they wanted to become a law enforcement officer. Like most, they said that they wanted to save lives and help their communities. Today, they would answer that question the same way. Their roles, however, have changed. Instead of directly performing law enforcement work, they direct the work of others. As such, they have the opportunity and obligation to direct they limited resources to tasks and activities that positively impact their communities.

Law enforcement leaders, whether local police chiefs, state troopers, or sheriffs, are faced with numerous, competing demands that include significant issues like increasing violent crime, home grown extremists, and opioid addiction. Given the seriousness and complexity of these problems, it is not hard to see why traffic safety sometimes takes a back seat. Law enforcement leaders should, however, consider the extent to which traffic safety impacts the overall safety of their communities. In 2015, there were 35,092 people killed in the U.S. in traffic crashes, a 7.2 percent increase from 2014 [1], while 15,696 were victims of homicide. [2] The number of victims in both of these categories is far too high, but the number of traffic crash victims is more than double the number of murder victims. For many of our communities, the odds of being killed or injured in a crash are far higher than suffering a similar outcome from a crime.

Citizens want to live in safe communities, and too often, safety is judged based on crime, particularly homicide. Many people consider large cities, where homicides occur in higher numbers, to be more dangerous than other places. However, in 2002, an article in *Governing* included an argument that safety is an issue broader than simply violent crime. The author asked, "What if, instead of being measured by itself, homicides were to be measured along with other forms of violent fatality, specifically, automobile crashes, the second major category of violent death in the United States?" William Lucy, a University of Virginia professor, found that the most dangerous parts of metropolitan areas are likely to be rural or exurban communities simply because the fatal crash rates are much higher. Lucy combined statistics for homicides committed by strangers and traffic fatalities from Houston, Texas, in 2000 and calculated a death rate of 1.5 per 10,000 people. Using the same calculation, he found that the rate in Montgomery County, Texas, bordering Houston, was 2.5 people, more than double the number in Houston. [3] This was due to the much higher rate of traffic fatalities. The point is that while violent crime makes the news, traffic crashes often present a greater threat. While there are some visible exceptions, most agencies could do more to improve the overall safety of their communities by ensuring that traffic safety is a continuous priority.

Hopefully, the safety of officers, troopers, and deputies is a high priority for law enforcement leaders as well as their agencies. Law enforcement officers drive millions and millions of miles every year, exposing them to all of the dangers associated with traffic crashes. A review of the Officer Down Memorial Page (ODMP) shows that traffic-related incidents are one of the leading causes of line-of-duty deaths. [4] Additionally, numerous more agency personnel are injured in these incidents. Consistently enforcing traffic laws and working to reduce crashes not only makes communities safer, it makes officers safer.

The economic costs of traffic crashes are tremendous. Here are some interesting and disturbing, findings from a 2010 publication of the National Highway Traffic Safety Administration:

- The economic cost of motor vehicle crashes that occurred in the U.S. in 2010 totaled $242 billion. This is equivalent to approximately $784 for every person living in the U.S. and 1.6 percent of the U.S. Gross Domestic Product.
- The lifetime economic cost to society for each fatality is $1.4 million. Over 90 percent of this amount is attributable to lost workplace and household productivity and legal costs.
- Each critically injured survivor cost an average of $1.0 million. Medical costs and lost productivity accounted for 82 percent of the cost for the most serious level of non-fatal injury.
- Lost workplace productivity costs totaled $57.6 billion, which equated to 24 percent of the total costs. Lost household productivity totaled $19.7 billion, representing 8 percent of the total economic cost.
- Total property damage costs for all crash types – fatal, injury, and property damage – totaled $76.1 billion and accounted for 31 percent of all economic costs.
- Congestion costs, including travel delay, added fuel usage, and adverse environmental impacts cost $28 billion, or 12 percent of total economic crash costs.
- Approximately 7 percent of all motor vehicle crash costs are paid from public revenues. Private insurers pay approximately 54 percent of all costs. Individual crash victims pay approximately 23 percent while third parties, such as uninvolved motorists delayed in traffic, charities, and health care providers, pay about 16 percent. Overall, those not directly involved in crashes pay for over three-quarters of all crash costs, primarily through insurance premiums, taxes, and congestion-related costs, such as travel delay, excess fuel consumption, and increased environmental impacts. In 2010, these costs, borne by society rather than by crash victims, totaled over $187 billion. [5]

Law enforcement leaders should also consider the amount of resources that their agencies devote to responding to crashes. If they can take action to prevent them, much like preventing crime, they can not only reduce the number of victims in their communities, but also re-allocate limited resources to other activities.

Keeping the roadways safe is a multi-disciplinary task that requires participation from law enforcement, engineers, emergency medical personnel, elected officials, advocacy

groups, and the general public. The individual roles of these groups include designing and maintaining roads in accordance with safety standards, developing effective laws and rules of the road, implementing response protocols to mitigate damage and injury when incidents occur, and ensuring comprehensive public awareness. While many of these overlap, there is one task that is exclusive to law enforcement, which is traffic enforcement. Law enforcement officers are sworn to enforce the laws, including traffic laws, and are given the authority to do so. In fact, they belong to the only profession that is granted this authority. It is incumbent upon them, therefore, to ensure that traffic laws are vigorously enforced to promote safe roadways.

The purpose of this article is to argue that the traffic stop is one of the most valuable self-initiated activities that a police officer, deputy, or trooper can perform, simply because a single traffic stop provides a high return on investment in the form of five separate benefits related to public safety.

Return on Investment

Specific Deterrence – Traffic: The most basic reason for stopping a vehicle is because of a traffic violation. The purpose of the stop is to identify the driver responsible for the violation and to take the appropriate enforcement action. Traffic citations and the penalties that may result are intended to change driver behavior. Even minor violations can result in hefty fines, higher insurance, and points against driver's licenses. If necessary, repeat offenders may have their licenses suspended or revoked by motor vehicle authorities who use conviction data to monitor the behavior of the drivers they license. This is particularly important for commercial vehicle drivers who operate the largest vehicles on the roadways, oftentimes across many states.

Studies have shown that highly visible traffic enforcement leads to reductions in traffic crashes and changes in driver behavior. For example, a study of the *Click It Or Ticket* Program in Massachusetts found that "tickets significantly reduce crashes and non-fatal injuries." [6] This, of course, is one of the underlying reasons for conducting enforcement in the first place.

General Deterrence – Traffic: The visibility traffic stops gets the attention of other drivers and have the potential to change their behavior as well. Passing drivers are likely to assume that a traffic stop is resulting in a citation for the other driver. That memory may help to change those drivers' behavior, particularly if the enforcement efforts are sustained over time.

A study sponsored by the National Highway Traffic Safety Administration (NHTSA) found that that "the most important difference between the high and low belt use states is enforcement, not demographic characteristics or dollars spent on media ... Enforcement was much more vigorous in the high belt use states, as shown by an average of twice as many seatbelt law citations per capita..." [7] There have also been a number of case studies documenting the effectiveness of high-visibility enforcement on impaired driving offenses. For instance, a formal evaluation of the Checkpoint Strikeforce program indicated a 7 percent decrease in impaired drivers involved in fatal crashes associated with the overall program. The participating states of Maryland and Virginia, as well as the District of Columbia, have all remained at low-fatality rates as the program has continued. [8]

Specific Deterrence – Crime: It is well-known that traffic stops lead to the apprehension of criminal suspects. Whether the offender is as notorious as the Oklahoma City Bomber or simply a wanted subject on a misdemeanor warrant, the violator contact can frequently lead to a criminal subject being arrested and the recovery of evidence, contraband, or illegal weapons. Any law enforcement officer that develops the skills to look beyond the traffic stop will consistently produce significant criminal arrests. For example, the Grand Prairie, Texas, Police Department determined that traffic enforcement was responsible for 37 percent of all arrests in 1994. It was also determined that 47 percent of the arrests made by traffic enforcement officers were for serious and criminal offenses. [9] This makes the traffic stop an indispensable tool in areas experiencing patterns or trends of criminal activity.

General Deterrence – Crime: Many criminals commit their crimes in areas where they are comfortable. This may be near their homes or places of work or recreation. The crime is made easier since the offender is familiar with the area, the people, and potential escape routes. If law enforcement can make an area uncomfortable for a potential criminal, the likelihood of a crime being committed may be reduced. What could be more uncomfortable than a police vehicle with lights flashing in the area of the potential crime?

Studies have shown that visible police presence has an impact on crime in targeted areas. Two studies in the 1970s and 1980s demonstrated that communities with higher levels of traffic enforcement also experienced lower rates of robbery. [10] In the mid-1990s, the Peoria, Illinois, Police Department dramatically increased its traffic enforcement and self-initiated activity. This resulted in large reductions in reported crimes, as well as traffic collisions. [11]

Since 2008, agencies around the country have been implementing the Data Driven Approaches to Crime and Traffic Safety (DDACTS) model to maximize the use

of resources to target both crime and crash problems. NHTSA states, "By identifying areas through temporal and spatial analysis that have high incidences of crashes and crime, DDACTS employs highly visible, targeted traffic enforcement to affect these areas. This model affords communities the dual benefit of reducing traffic crashes and crime, thus reducing overall social harm. Drawing on the deterrent value of highly visible traffic enforcement and the knowledge that crimes often involve the use of motor vehicles, the goal of DDACTS is to reduce the incidence of crashes, crime, and social harm in communities across the country." [12]

Research suggests that this has been successful. A study of the Shawnee, Kansas, Police Department's use of DDACTS found reductions in robbery, auto theft, and auto burglary, along with total reductions in targeted crimes of almost 40 percent over a three-year period. Overall crashes were also reduced by 24 percent. [13]

Intelligence: Perhaps the most valuable benefit of the traffic stop is the information that it generates. Gone are the days when citations and warnings were simply filed away. Modern records management systems allow us to collect information about who is stopped, what they were driving, where it occurred, and when it happened. This information can be extremely valuable to the investigation of crimes that may not have been discovered at the time of the stop. Crime analysts and investigators use this information to develop suspects and leads that may result in the clearance of criminal incidents.

All of this results in a tremendous return on investment from a single traffic stop carried out by uniformed patrol personnel. For these reasons, law enforcement leaders should be doing everything possible to encourage traffic stops in their communities.

A simple way to start a discussion about traffic stops with enforcement personnel is to talk about tolerance; in other words, under what circumstances do officers routinely stop vehicles? Law enforcement leaders should this question in a room full of officers. The answers will vary greatly, ranging from hazardous violations and suspected crimes, to administrative violations, such as expired tags. While officers have always had and will continue to have discretion in terms of stopping vehicles, command staff should encourage stops for all of these things. The discussion gets better when the topic of speed tolerance is introduced. An officer will rarely admit to stopping a speeding vehicle for less than 10-20 miles per hour over the limit. This begs the question of why they would allow drivers to routinely violate established speed limits by this margin, particularly in residential areas, school zones, or high crash areas. Law enforcement agencies should be working to lower this tolerance to enhance the safety on roadways, pointing out that the mere stopping of a vehicle does not necessitate charges being placed.

While this resource guide strongly advocates for traffic enforcement, it should be done in a random or arbitrary manner; should be purpose-driven and directed at social harms affecting our communities.

Enforcement Done Right

Communities expect their law enforcement agencies to keep the population and their roadways safe. In other words, they expect, and sometimes demand, traffic enforcement. Any law enforcement official who works with residential communities can recount the numerous, and sometimes vociferous, complaints of speeding and other local traffic violations that are brought to their attention by citizens. These citizens rightly expect that, when complaints are valid, their local law enforcement agency will take action. They also expect that their children can travel safety to and from school and their daily commutes, and those of their family and friends, can be completed in a timely and safe manner. While enforcement practices in some areas have led to criticism, the fact remains that a strong traffic safety program is integral to community policing.

The return on investment from the traffic stop becomes especially significant when the activity is deployed properly. Enforcement should be purpose-driven and directed at a specific problem occurring in a community. For the most part, these problems will relate to traffic crashes, crime, or other social harms. It is important to understand where problems are occurring, as research has shown that a large percentage of criminal incidents occur in relatively small geographical areas.

The first major study to arrive at this conclusion was conducted in Minneapolis in the 1980s. The study found that 3.5 percent of the addresses in the city of Minneapolis produced about 50 percent of crime reports. Another study in Seattle found that 86 street segments out of over 29,000 examined accounted for one-third of juvenile crime in the city. [14] Observations would suggest that this also occurs for traffic crashes as state highway safety offices and law enforcement agencies routinely analyze the locations of crashes and identify areas and intersections with particularly high numbers of incidents. Deploying enforcement to the places where problems occur is the first step towards mitigating the dangerous effects of traffic violations. Of course, narrowing this further, targeting the days and times when the problem is most likely to occur will also increase effectiveness. Officers engaged in targeted enforcement should understand what they are doing and why. While it is appropriate to expect that officers will enforce violations that they observe while on routine patrol, there should be a reason for targeted

enforcement and officers should understand it. It is even better when officers communicate that reason to the drivers being stopped. A data-driven, place-based, and purpose-driven approach is appropriate and provides the information necessary not only to justify actions, but also to share with their communities to promote understanding.

To be accepted by their communities, enforcement must not only be data-driven and place-based, it must also be conducted in a legally sound, fair, and impartial manner. Simply driving around a vehicle in a high-crime or high-crash area is not, by itself, a reason for a stop. Over the years, there have been many court decisions that define what is required for a stop to comply with constitutional principles. Generally, the totality of the circumstances must lead to "a particularized and objective basis for suspecting the particular person stopped of criminal activity."[15] This is the basis for reasonable suspicion, which is necessary before a stop is made. Fortunately, most traffic stops are made for observed violations of traffic laws and far exceed the criteria established by the Supreme Court. Officers should be cautioned, however, that initiating a stop for suspected criminal activity may require a more specific articulation of facts.

Fairness and consistency is a critical part of any enforcement program. The notion of fairness is imbedded in the principles of procedural justice. Leading researchers on this topic have identified several factors that influence the perception of fairness:

- **Voice:** The perception that your side of the story has been heard.
- **Respect:** The perception that system players treat you with dignity and respect.
- **Neutrality:** The perception that the decision-making process is unbiased and trustworthy.
- **Understanding:** Comprehension of the process and how decisions are made.
- **Helpfulness:** The perception that system players are interested in their personal situation to the extent that the law allows. [16]

Most of these factors can be achieved through communication with the person being stopped. Although officers may never be able to change the perception of some who simply refuse to understand the role of law enforcement, the overwhelming majority of citizens will respond positively to officers who provide an explanation for the stop and what will happen as a result.

Fairness is particularly important as it relates to the disposition of a stop. Violators should be treated as similarly as possible based on the seriousness of the offense. Officers have the discretion to use enforcement options that range from physical arrest to warnings. The use of these should be proportional to the offense, with more serious and hazardous violations resulting in more severe actions. Fairness naturally leads to the need for consistency. Agencies should consider policies and training that define enforcement options and their suggested uses. In general, officers have the following options:

- **Physical Arrest:** Physical arrest is the most severe enforcement option available and is appropriate for serious violations, which are generally prescribed in the laws of each state. Significant traffic violations, such as impaired driving, often result in arrest. Criminal examples would include outstanding warrants or possession of illegal weapons or controlled substances.
- **Citation:** Citations, normally resulting in a monetary fine or points against a driver's license, may be the most common form of traffic enforcement activity. These are appropriate for hazardous traffic violations, particularly those that are contributing to traffic crashes in targeted areas. Other appropriate uses would include significant administrative violations such as lack of a license, suspended driving privileges, driving without insurance, and significant registration issues. One other area where citations are almost always appropriate is occupant protection. Seatbelt use in most states has been mandatory for many years. Those who violate these laws are likely to be doing so intentionally; therefore, enforcing these laws by issuing citations is appropriate.
- **Written Warning:** Many agencies use or have recently implemented written warning systems. These are based on the premise that the appropriate response to a violation is not always a formal enforcement action. Violations that are minor in nature or are newly enacted may be handled more effectively as an educational opportunity for the motorist. The purpose of using a written warning is to document the nature of the stop and maximize the benefits that have previously been discussed. Appropriate uses of this tool may include minor or less-hazardous moving violations, administrative issues such as expired tags, and speeding violations where the motorist is only slightly above the posted limit.
- **Verbal Warning:** Verbal warnings have existed for as long as traffic stops. Even in agencies without formal written warning policies, these are being used. It is simply a function of officers trying to achieve fair outcomes in their enforcement stops. When written warnings are allowed, verbal warnings should be minimized as they don't result in a record of the stop. There will always be a few cases where these

are appropriate, such as the need to respond to an emergency call after a stop has been initiated.

It is important that agency leaders take the time to consider policies and training related to the importance of traffic enforcement, procedures for traffic stops, and appropriate outcomes. The New Jersey State Association of Chiefs of Police has developed a model policy entitled "Traffic Enforcement Tolerances and Latitude" that addresses these issues. It also discusses a variety of violations and enforcement options to ensure fair and consistent enforcement. It does not, however, supplant an officer's judgement or discretion in dealing with the myriad of issues that can arise from a stop.

Much of the external and internal issues that traffic stops have been known to cause could likely be avoided by having simple conversations about these issues. Our employees and our communities should understand what we do and why we do it. This can be accomplished with a little planning and good communications.

Conclusion

There is and always has been a strong case for making traffic safety a priority and using traffic enforcement as a tool to reduce both traffic crashes and crimes. Doing this the right way takes time to plan and properly implement. Fortunately, there are numerous resources that can help. Consider the following:

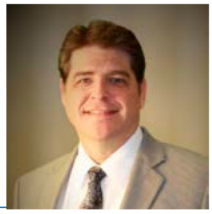
- Every state has a highway safety office that is responsible for distributing highway safety grant funding. Many of these offices have law enforcement liaisons and other staff and resources for the specific purpose of helping agencies implement traffic safety programs. A list of state offices as well as other highway safety resources can be found here: http://www.ghsa.org/about/shsos
- The National Highway Traffic Safety Administration maintains a web site with a tremendous amount of information on all aspects of traffic safety here: https://www.nhtsa.gov/road-safety .
- The IACP posts a variety of related information on its web site at: http://www.iacp.org/TrafficSafety
- Many state chiefs and sheriffs associations can also help. For example, the Virginia Association of Chiefs of Police coordinates the "Smart, Safe, and Sober" Program here: http://www.smartsafeandsober.org/. The Maryland Chiefs of Police Association, Maryland Sheriff's Association, and the Maryland Highway Safety Office recently collaborated on the publication of the "Law Enforcement Executive's Guide to High Visibility Enforcement," which can be found here: http://www.nlelp.org/wp-content/uploads/2016/09/LE_Exec_Guide.pdf

These resources will help law enforcement leaders focus on traffic safety and improve the safety of their communities.

Notes:

1. https://www.nhtsa.gov/press-releases/traffic-fatalities-sharply-2015
2. https://www.nytimes.com/2016/09/27/us/murder-crime-fbi.html
3. http://plannersweb.com/wp-content/uploads/2006/10/297.pdf
4. http://www.odmp.org/
5. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812013
6. Luca, Dara N. "Do Traffic Tickets Reduce Motor Vehicle Accidents? Evidence from a Natural Experiment," Journal of Policy Analysis and Management, Vol. 34, Issue 1, Winter 2015.
7. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/810962
8. https://www.nhtsa.gov/staticfiles/nti/pdf/811716.pdf
9. http://acrs.org.au/files/arsrpe/Paper%2029%20-%20Fell%20-%20Traffic%20Leg%20&%20Enforcement.pdf
10. http://acrs.org.au/files/arsrpe/Paper%2029%20-%20Fell%20-%20Traffic%20Leg%20&%20Enforcement.pdf
11. http://www.tiami.us/wp/wp-content/uploads/2013/01/the_peoria_experience.pdf
12. https://www.nhtsa.gov/staticfiles/nti/ddacts/811185_DDACTS_OpGuidelines.pdf
13. Bryant, Kevin M., Greg Collins, and Josie Villa. "An Evaluation of Data Driven Approaches to Crime and Traffic Safety in Shawnee, Kansas, 2010-2h013." Washington, DC: Bureau of Justice Assistance, Smart Policing Initiative, 2014.
14. Weisburd, David. "Place Based Policing," Ideas in American Policing. Police Foundation: Number 9, January 2008.
15. United States v. Cortez, 449 U.S. 411 (1981)
16. https://cops.usdoj.gov/html/dispatch/09-2013/fairness_as_a_crime_prevention_tool.asp

Leading Traffic Safety



By: **Dr. Mitchell Weinzetl,** *Former Senior Program Manager,* The International Association of Chiefs of Police

If you do a quick Internet search on *negative articles about the police*, you will get about 61 million hits. In the wake of such negativity, some law enforcement leaders (and some police officers) have questioned the value of continuing proactive traffic stops.[7] In addition, various members of the public and the media have even suggested that police agencies should rethink this aspect of their work, calling for a reduction or elimination of traffic stops altogether.[8] Although those involved in the discussion have offered numerous reasons for considering a reduction of effort in this area, much of the emphasis seems to focus on reducing biased enforcement. To be clear, biased policing is wrong, in any category. Still, from an industry leadership

7 http://www.npr.org/2016/07/25/486945181/some-police-departments-are-rethinking-traffic-stops-to-reduce-bias
8 http://www.latimes.com/opinion/op-ed/la-oe-0813-kutz-traffic-stops-20150812-story.html

and public safety perspective, the question remains; "Is reducing traffic enforcement or the use of traffic stops in everyone's best interests?"

According to the National Highway Traffic Safety Administration (NHTSA), there were 35,092 fatal motor vehicle crashes in 2015, which represents a 7.2 percent increase over 2014 figures.[9] The number of fatal crashes in 2015 translates into 96 fatalities per day, with one occurring every 15 minutes across the U.S. In the same year, NHTSA estimates that there were 2,443,000 injuries associated with motor vehicle crashes, which amounts to nearly 5 persons injured in crashes per minute, in every hour of every day. In light of these statistics, it is evident that traffic safety is an ongoing concern in the U.S., and despite criticism over their use, law enforcement leaders need to remain vigilant in encouraging the use of traffic stops to achieve public safety objectives. However, leaders also have the responsibility to ensure that traffic stops are done properly, in an unbiased manner, and that their use and purpose is clear, both to the officers who conduct them, and those in the public who are on the receiving end of these encounters.

Most would agree that the primary purpose of a traffic stop is to "promote public safety by stopping a violation, reducing crashes [the severity and number], and enhancing public enjoyment."[10] Significant private and public research has been done regarding traffic stops and roadway safety (e.g., NHTSA, Bureau of Justice Assistance), and there is significant evidence that there is a correlation between traffic enforcement and reducing motor vehicle crashes. In particular, a 2015 study that evaluated the *Click It Or Ticket* campaign in Massachusetts, showed that a 1 percent increase in traffic citations resulted in a .28 percent reduction in traffic crashes.[11] In one specific example, Safe Communities of Wright County Minnesota, which is a private collaborative traffic safety partnership focused on the areas of Enforcement, Education, Engineering and Emergency Medical Services (the 4 E's), has observed a 40 percent reduction of serious injury and fatal motor vehicle crashes since 1997, all of which occurred during a period of significant population and traffic growth within the county.[12] Although there is clear evidence that supports the importance of traffic enforcement in reducing motor vehicle crashes and promoting public safety, some still object to their use, and it is important to understand what is prompting these objections.

Despite the significant evidence that supports the use of traffic stops in improving roadway safety, traffic stops have also become a popular tool by the police in addressing issues of crime, particularly drug trafficking. In fact, there are a variety of resources available for officers that encourage the use of traffic stops for detecting criminal activity, including Charles Remsberg's ageless text, *Tactics for Criminal Patrol*, and numerous in-service training courses on criminal interdiction through traffic enforcement. Like the traffic safety data, regular media reports that chronicle significant arrests emanating from traffic stops, provide significant evidence of the effectiveness of these efforts. Even though these approaches work, *success* in this regard (in terms of arrests) has caused great scrutiny over the tactics used, and whether they are biased or discriminatory.

As criminals have become more sophisticated and as crime has evolved, law enforcement has evolved, too. Recognizing that catching criminals, and preventing and solving crimes, is a complex business, much of the policing industry has turned toward intelligence-led policing,[13] predictive policing,[14] or data-driven approaches to policing. These methods involve an analysis of data available to the agency to determine personnel deployments, to include proactive efforts in hot-spot areas (where crime is notably higher or more frequent than other areas) or areas where predictive models suggest a greater likelihood of criminal incidences. However, this data analysis is not necessarily restricted to crimes, it also typically involves an analysis of traffic patterns areas where a significant number of motor vehicle crashes occur.

In an effort to engage best-practices relating to the use of data, many law enforcement agencies have adopted a specific operational model, Data-Driven Approaches to Crime *and* Traffic Safety (DDACTS).[15] The DDACTS model utilizes "location-based traffic crash and crime data to establish effective and efficient methods for deploying law enforcement and other resources." One of the key components of the DDACTS model is the strategic and tactical focus on places. This focus is based on three underlying assumptions:

- It is more efficient to focus on places than to focus on individuals;
- The places that experience a high number of traffic crashes also exhibit a high number of crimes; and

9 https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812318
10 https://www.criminaljusticedegree.com/basic-composition-of-traffic-enforcement/
11 Luca, D. L. (2015), Do Traffic Tickets Reduce Motor Vehicle Accidents? Evidence from a Natural Experiment. J. Pol. Anal. Manage., 34: 85–106. doi:10.1002/pam.21798
12 https://www.safecomm.org/
13 https://www.ncjrs.gov/pdffiles1/bja/210681.pdf
14 https://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/welcome.aspx
15 https://www.nij.gov/topics/law-enforcement/operations/traffic/Pages/ddacts.aspx

- Tools like computer mapping have made it easier to adopt place-based strategies.[16]

The use of DDACTS (or other data-driven approaches) by police agencies is a double-edged sword; the methods used produce positive results, but they can also produce community trust and resentment issues by those who feel disaffected. Accordingly, it is incumbent upon law enforcement leaders to address and mitigate these concerns. So, what should law enforcement leaders do?

1. Law enforcement leaders must understand that there is a right way (and a wrong way) to conduct traffic stops. Most in the industry would agree that traffic stops have the potential to be dangerous and contentious, and officer-safety issues demand that they are conducted in a particular manner. At the same time, concerns over officer safety do not necessitate that officers engage in behaviors that are considered rude or abrasive, and leaders should not condone this or accept this as a given or an excuse by officers. Traffic stops can be done correctly, safely, and frequently, without generating citizen complaints. For example, Los Angeles Sheriff's Deputy Elton Simmons has written more than 25,000 traffic tickets over 20 years, all without generating a single complaint.[17] The Elton Simmons YouTube video, provides a real-life example of how the approach and demeanor of the officer can contribute to success in the traffic safety mission. This video could be a valuable training tool for new officers, or those who seem to generate an inordinate number of complaints. Either way, leaders must set the standard for traffic stop encounters, and leaders must provide staff with the guidance they need to conduct them properly, safely, and in an appropriate manner.
2. Leaders should ensure that officers understand that during all traffic stops, they are expected to engage the elements of *Procedural Justice.*[18] As noted in the 21st Century Policing Task Force Report, the core concepts of procedural justice include:
   - Treating people with dignity and respect
   - Giving individuals 'voice' during encounters
   - Being neutral and transparent in decision making
   - Conveying trustworthy motives

   Although the concepts should be promoted throughout the organization, internally and externally, and with respect to all citizen contacts, the frequency and nature of traffic stops requires that officers consistently practice these behaviors. Additionally, leaders should develop strong policies related to impartial policing, and provide ongoing training to officers in these areas, whether that training is formal or informal.
3. When considering concentrated enforcement efforts, whether they relate to traffic safety, crime, or both, agencies should be data-driven, to include monitoring of resources deployed, and the results of those efforts. Part of the data-led strategy of the agency should include examining whether their tactics are producing required results, and if they are not, leaders should thoughtfully adjust their approach. Leaders should share this information and the results with the public, to include outcomes, and any associated adjustments in the approach of the department.
4. Whether traffic stops are used for crash reduction or crime interdiction, leaders should adopt an education strategy, both for officers, and for the public. Officers need to understand where they are being deployed and why, and what their objectives are. They also need to understand the purpose behind what they are being asked to do, as this will equip them to engage the public in a positive manner. Agencies should consider creating a literature piece that explains why they are conducting traffic stops, or working a criminal interdiction detail. Officers could use this brochure as a means to explain their presence, and to further justify the intervention. This type of action relates back to procedural justice, and adds to police transparency and legitimacy.
5. In addition to delivering materials during direct encounters, agencies can also educate the public in other ways. Many police agencies use various social media outlets, such as Facebook and Twitter, to convey important public safety messages. Some departments, like the Orwell, Ohio, Police Department, have even used their website as an educational forum, providing detailed information about why the police make traffic stops, why the police act in a certain way during those encounters, and tips on what the public can do to make the traffic stop less stressful for all.[19]
6. More than ever in the history of law enforcement in the U.S., there is a need for leaders to engage the public directly on the issues of crime, police procedures, and

16 https://www.nhtsa.gov/staticfiles/nti/pdf/809689.pdf
17 https://www.youtube.com/watch?v=Phzi1wmEeEw (Elton Simmons)
18 The President's Task Force for 21st Century Policing, *Final Report of the President's Task Force for 21st Century Policing* (Washington, D.C.: Office for Community Oriented Policing Services, 2015), http://www.cops.usdoj.gov/pdf/taskforce/TaskForce_FinalReport.pdf
19 http://www.orwellpolice.com/trafficstops.htm

personnel deployments. The public has a keen interest in what the police do, as those efforts tend to affect them, either directly or indirectly. Further, the public has set a new standard of accountability for the police, and more transparent and robust communication is now a mandate. When police agencies are considering new or varied approaches to crime and/or traffic safety, leaders should thoughtfully consider how these strategies will affect the public, and when doing so would not compromise those efforts, the public should have the opportunity to offer their feedback and input for consideration.

Traffic stops have proved to be a very effective mechanism for police agencies to improve roadway safety, and to reduce crime and apprehend criminals. In conducting traffic stops, it is important, that law enforcement leaders ensure that traffic stops are done properly, for the right reasons, and in a fair and unbiased manner, which does not produce discriminatory treatment.

Secondary to ensuring that they are done properly, law enforcement leaders also have a responsibility to engage the public on this topic to explain the purpose, processes, and personnel deployments used, and to educate the public on the outcomes associated with these efforts. Further, in keeping with a procedural justice approach, police agencies should consider allowing the public to have a voice in this process, when appropriate, and law enforcement leaders should consider the will of the public when determining how, when, and where, the police engage the resources at their disposal.

In Pursuit of Bias-Free Traffic Enforcement



By: **Lorie A. Fridell, PhD,** *Associate Professor,* Department of Criminology at the University of South Florida

The issue of biased policing returned to the forefront in the late 1990's and early 2000's. The focus was on vehicle stops and we heard complaints about "Driving while Black" and "Driving while Brown." The issue of biased policing returned to the forefront *again* in 2014 following the shooting of Michael Brown and other events in Ferguson, Missouri. Attention turned to bias and the use of force, but again vehicle stops remained in the headlines; many of the most controversial cases involved police actions associated with a vehicle stop, including incidents in Cincinnati, Ohio; North Charleston, South Carolina; Columbia, South Carolina; Waller County, Texas; and Tulsa, Oklahoma.

This article will focus on bias in policing, with a particular emphasis on both the issues and interventions as they are linked to traffic enforcement. It will address the topic using the perspective of the modern science of bias that recognizes that even well-intentioned individuals, including well-intentioned law enforcement, have biases that can impact on perceptions and behavior. After setting forth the science and discussing how bias might manifest in traffic enforcement, the article will outline what agency leaders can do to promote bias-free policing in traffic enforcement and all other police activities. Emphasis will be given to interventions linked to training and measurement.

The Modern Science of Bias

Social psychologists have been studying bias and prejudice since about the 1950's. For a long time, they recognized only what we now call "explicit biases." With explicit biases, a person associates groups–such as racial minorities, women, transgender individuals, homeless people–with negative stereotypes. These associations are based on animus or hostility toward the groups, and the person with these biases is well aware of them and unconcerned about the discriminatory behavior that those biases produce. (See, e.g., Amodio & Mendoza, 2010; Dovidio et al., 1997; Nier, 2005; Petty, et al., 2009). As an example, a racist has explicit biases.

Starting in the 1980's, these social psychologists discovered another way that bias and prejudice can manifest–in the form of *implicit* biases. Implicit biases share some similarities with explicit biases. With implicit biases, we still link individuals to stereotypes or generalizations associated with their group or groups. And these biases and stereotypes can impact on perceptions and behavior. But, unlike explicit biases, implicit biases are not based on animus or hostility and these implicit associations can impact individuals *outside* of conscious awareness. The worst news is that, even individuals who reject prejudice and stereotyping at the conscious level, can and do manifest implicit biases (Correll et al., 2007; Dasgupta, 2004; Dovidio, et al., 2002; Dovidio et al., 2009; Greenwald & Krieger, 2006).

This science requires that we move away from the "old notion" that individuals who produce biased policing are identifiable by their overt animus and hostility toward groups. We now know that even our well-intentioned law enforcement professionals can produce biased policing. In fact, the key implications for law enforcement of the science of implicit bias are these: (1) even the best officers—because they are human—can produce biased policing; and (2) even the best agencies—because they hire humans to do the work–will have biased decisions and therefore must be proactive to produce fair and impartial law enforcement.

How Bias Might Manifest in Law Enforcement?

How might implicit bias manifest in law enforcement? It may lead an officer to perceive the ambiguous behavior of a Black male as more threatening than the same behavior on the part of a White male. It may manifest among agency command staff who decide (without crime-relevant evidence) that the forthcoming gathering of Black college students bodes trouble, whereas the forthcoming gathering of White undergraduates does not. Although these types of implicit biases pertaining to Blacks and crime are well-documented, there are other biases that might impact law enforcement actions or procedures. For instance, implicit bias might lead an officer to be consistently "over vigilant" with males, low-income individuals, and Hispanics, and "under vigilant" with female subjects, people of means, and Asians.

Traffic enforcement is "ripe" for the manifestation of implicit biases. First, most people's interactions with police is in the context of traffic enforcement. Second, there is lots of discretion in traffic enforcement, and wherever there is discretion there is the potential for human bias. Putting those two facts together, we have interactions that are both numerous and at high risk for human bias.

How might implicit bias manifest in traffic enforcement?

Implicit bias might lead the line officer to automatically perceive crime in the making when he or she observes two young Hispanic males driving in an all-Caucasian neighborhood. When there is a motor vehicle crash and the participants tell two different versions of what happened, implicit bias might lead the trooper to believe the story of the man in the shirt and tie driving the BMW as opposed to the story of the man in dirty jeans driving a pick-up truck. After a vehicle is stopped, implicit bias might lead the deputy to request for consent to search from the young kids in low-hanging pants, whereas the same request would not be made of individuals with other demographics and dress.

Consequences of Biased Policing

There is no question that biased policing can negatively impact the community members who are on the "receiving end" of this treatment; and those negative experiences can produce negative impressions of law enforcement that can have serious consequences for agencies (Tyler & Huo, 2002). But it is also the case that biased policing can have negative *impacts on the officer engaged in it.* Policing based on biases or stereotypes can produce ineffective, unsafe, as well as unjust policing. In terms of *effectiveness*, biases and stereotypes might, for instance, lead an officer to focus on a particular group in her surveillance or when she runs queries on license plates (see Meehan & Ponder, 2002). If this focus is link to stereotypes about demographic groups and not criminal intelligence, she might miss the traffic violations or crimes committed by other demographic groups to which she does not attend. In a role play in the training program described below (Fair & Impartial Policing), patrol officers are dispatched in a role play to a domestic violence scene and told the perpetrator is still present. They arrive to find the sobbing victim with a man comforting her on one side and a woman comforting her on the other. Invariably the officers approach the man and take him off to the side–leaving the victim next to the actual perpetrator, the female partner. Biases can lead to *ineffective* policing.

Policing based on stereotypes and biases can also be *unsafe*. Much of the community concern about bias since the events in Ferguson has pertained to use of force. The allegation is that law enforcement are over-vigilant with certain groups based on stereotypes about that demographic. (An example is provided below.) But the converse of this potential problem is the danger when police are *under-vigilant* with certain groups based on their biases. Correll et al (2002, 2007) in laboratory "shoot, don't shoot" studies found that both police and non-police subjects were slower to identify a gun in the White man's hand, than in the Black man's hand. The danger of biases leading to under-vigilance was highlighted in a story shared by an officer with the Las Vegas Metropolitan Police Department.[20] This officer was responding to the shooting of two of his fellow officers in 2014. The PD knew little about who had shot these officers, but other events indicated they might be inside a nearby Walmart. The officer telling the story was moving down a Walmart aisle toward a White male that he identified as the killer of his colleagues, when he saw a White female. He reports, "I thought that this woman wasn't going to be a threat and so I let her remain as she was a little bit longer than I should have." Once he realized that she "wants to be exactly where she is right now," he exchanged gunfire with her, wounding her and thwarting the threat. (He was not hit.) In telling his story, this officer recognized that his (very understandable) stereotypes about who is a threat slowed down his response and could have led to his own death.

An additional concern about how biases can be unsafe for police was raised in the New York State Task Force on Police-on-Police Shootings (2010). This Task Force found for both the state and the U.S. that the off-duty, plain clothes officers who were the tragic victims of friendly

20 The story was shared during a segment entitled "Cops See it Differently, Part 2" on "This American Life" broadcast February 13, 2015. Found on 3/20/2017 at https://www.thisamericanlife.org/radio-archives/episode/548/cops-see-it-differently-part-two; segment starts at 54:00.

fire were disproportionately individuals of color. The Task Force writes (2010, p. 3): "Our conclusion from the review is clear; inherent or unconscious racial bias plays a role in shoot/don't-shoot decisions made by officers of all races and ethnicities. The role may be small and subtle, measured during simulations only in milliseconds of action or hesitation, but the patterns . . . are clear and consistent."

Policing based on stereotypes and biases can also be *unjust*. An incident involving a South Carolina Trooper raises the specter of bias impacting on an officer's decision to shoot. In-car cameras show Trooper Sean Groubert pulling over a young man for a traffic stop. They both pull into a gas station and stop their cars. The young man of color emerges from his car and is asked by the trooper to produce his license and registration. The young man turns quickly to reach into the car and the trooper– his on-camera voice clearly indicating fear–opens fire on the man, hitting him in the hip. While it is perilous to try to ascertain motivations, including biased motivations, it is legitimate to ask whether a middle-aged woman engaging in the same behavior would have produced the fear and gunfire on the part of this trooper.

Promoting Bias-Free Policing Through Training

With the assistance of the modern science of bias, the law enforcement profession can be more effective in the efforts to promote bias-free policing. We certainly cannot stop the efforts that agencies have adopted to combat manifestations of *explicit bias*. For instance, agencies try to screen out individuals with explicit biases at the hiring stage; agency leaders try to identify officers with explicit bias (who were *not* screened out at the hiring stage) to hold them to account. The discovery of implicit bias, however, requires that our efforts be more comprehensive. What agencies can do to promote bias-free policing comes under the heading of a "comprehensive program to produce fair and impartial policing." Interventions within the "comprehensive program" are linked to these elements (see Fridell 2017):

- leadership and culture,
- recruitment and hiring,
- bias-free policing policy,
- training,
- supervision,
- accountability,
- measurement,
- outreach to diverse communities, and
- operations.

Highlighted here are guidance for agencies in the realms of training and measurement.

There are two types of training programs for law enforcement that reflect the modern science of bias: (a) implicit bias awareness training and (b) high-quality, scenario based use-of-force training.

Implicit Bias Awareness Training

For many years, across the U.S., traditional "racial profiling" training has missed the mark because some programs were based on outdated understandings of bias and prejudice. Many of these programs have treated the law enforcement audience as if they all manifested explicit bias. The message was that police needed to "stop being prejudiced," with an emphasis on reducing police animus toward marginalized groups. We now know that this message is ill-suited to most law enforcement, who may not hold explicit prejudices. And further, these messages–offensive to most–have produced a backlash against training linked to this topic.

For the overwhelming majority of well-intentioned officers who want to police safely, effectively and justly, the training that is needed is "implicit bias awareness training." Such programs give officers the information they need to recognize their implicit biases and also, importantly, give them the tools to reduce and manage them. These programs use curricula that address not just racial or ethnic bias, but also biases based on other factors such as sexual orientation, gender identity, socio-economic status, gender, and so forth.

The Fair & Impartial Policing (FIP) Training Program (www.fairandimpartialpolicing.com) was developed with the assistance of law enforcement experts and social scientists, and with the financial support of the USDOJ Office of Community Oriented Policing Services (COPS Office). There are specific curricula for various subsets of agencies: (1) recruits in the academy and patrol officers, (2) first-line supervisors, (3) mid-level managers, (4) command-level personnel, and (5) trainers (i.e., the train-the-trainer version).

The mantra of the curriculum for academy recruits or in-service patrol officers is: "policing based on stereotypes and biases is ineffective, unsafe, and unjust." Trainees learn (1) about the science of bias, (2) how individuals can reduce and manage their biases, (3) how impartial policing is linked to the concepts of procedural justice and legitimacy, and (4) what they need to do as police professionals to ensure bias-free policing.

First-line supervisors and mid-level managers, like the patrol officers, need to understand the science of bias and the tools for reducing and managing them. However, these groups also need to understand how to "scan" for biased policing on the part of their subordinates and how

to intervene when bias is suspected. It is made plain during the training that identifying biased behavior is not easy, because "biased policing" is, by definition, linked to the motivations of the officer. The training program guides supervisors on when and how they can (and should) intervene to stop what *appears* to be inappropriate conduct, while keeping in mind the ambiguous nature of the evidence and the sensitive nature of the issue. The newly updated 2017 version trains supervisors to engage in "crucial conversations" (Patterson et al., 2012) and discusses how biases can manifest *internal to the agency* in the form of "managerial bias."

The command-level FIP curriculum is arguably most effective when the agency executive invites concerned community stakeholders to participate. Full-group and small-group discussions allow participants to share their views; perspectives; and, sometimes, their long-held frustrations. Together they learn about the implications of the science of bias for police policies and practices. This program covers the previously mentioned "comprehensive program to produce fair and impartial policing." After participating in the program, police executives come away from the training with preliminary action plans.

Importantly, implicit bias awareness curricula do not have to, indeed *should not*, ignore the elephant in the room. It is a criminological fact that some demographic groups engage disproportionately in some types of crimes. White individuals are disproportionately represented among people involved in crimes of the powerful (see e.g., Lynch & Michalowski, 2006) and people of color are disproportionately represented among people who commit street crimes (see e.g., Kubrin & Weitzer, 2003; McNulty & Bellair, 2003; Sampson et al., 2005). That these disparities exist does not negate the existence nor harm of implicit biases. It is time to bury the false narrative that there is *either* (a) disparity in criminal behavior across demographic groups, or (b) police bias. There can be both.[21]

These training sessions can produce a transformation in thinking among participants. It is not unusual, in fact it is common, for attendees to enter the room for Fair & Impartial Policing training with attitudes that are defensive or even hostile. They may expect another program that treats them as if they all have explicit biases. But then the trainers start to talk about science; and it is not the science of *police* bias, it is the science of human bias. The attendees start to learn about how their human biases might make them unsafe, ineffective and unjust, and the defenses start to melt away. Comments in evaluations include:

- **Recruit Participant:** *I learned what 'implicit bias' means and understand its effects on me, (the) decisions I make and (the) community perceptions of officers.*
- **Patrol Officer Participant:** *We were told we were going to 'racial profiling' class all day and, to be honest, that already put me off–thinking it was going to be the same stuff we always get. I was very, very surprised and happy to receive this training today.*
- **Mid-level Manager Participant:** *(The training) gave me some eye-opening information. I used to say I wasn't biased; I can no longer say that. However, this course has given me the opportunity to have an open conversation about this topic.*
- **Command-level Participant:** *I am leaving the class with a new perspective on my own views and beliefs. I have a new awareness of bias-based policing within my own agency. The presentation of scientific data provided me with a more convincing argument that supported the existence of unintentional, but widespread racial bias, which I was typically quick to dismiss.*
- **Training-of-Trainers (TOT) Program Participant:** *(I) wanted nothing to do with FIP or its philosophy. As fate would have it I was "hand-picked" to attend the (train-the-trainer) classes and forced to go after presenting every excuse I could come up … I came in Monday as opposed and defensive as I could covertly be without getting into trouble…. It took about two hours and I was sold on the theory of the class and wondering why I had not been through this training sooner.*

High-Quality, Scenario-Based Use of Force Training

The implicit bias awareness training described in the previous section is most relevant for those decisions where the law enforcement professional has a moment, even a brief one, to contemplate how his or her biases might be impacting on him/her. The program helps them recognize when implicit biases might be manifesting and helps them to thwart their impact on behavior. Some police decisions, however, do not allow for that moment of contemplation. This is especially true of often quick-moving use-of-force situations. To help thwart the impact of human biases on these split-second decisions, agencies need to provide scenario-based, use-of-force judgment training that conditions officers to focus not on demographics, but on indicators of threat. The implicit bias concept—exposure to counter-stereotypes (see e.g., Blair et al., 2001; Dasgupta & Rivera, 2008)—can be used to explain the potential of this bias-reducing training. In modern, state-of-the-art, use-of-force training, officers "role play" while interacting with one or more individuals in video scenarios. The officer must determine whether or not the person in the scenario is a threat and, if the

21 Agency policy on biased policing is important for communicating clearly to personnel when it is legitimate, and when it is not, to consider demographics in making law enforcement decisions. See Fridell 2017.

person *is* a threat, the appropriate amount of force to use. This raises the question: How might effective use-of-force training take the demographics—and associated stereotypes and biases—out of that decision-making? The answer is as follows: The individuals who turn out to be a threat in a given scenario must be just as likely White as Black, just as likely female as male, just as likely old as young, and so forth. With prolonged exposure to these counter-stereotypes over time, the law enforcement officer should learn that demographics are "non-diagnostic" in terms of threat, and the officer should instead redirect his focus to different clues, such as placement of hands and other subject behavior. Laboratory studies indicate the potential value of this exposure for removing the effect of demographics—and the associated stereotypes—from split-second decisions regarding the use force (Plant et al., 2005; Plant & Peruche, 2005).[22]

Numerous agencies use video scenarios for their use-of-force judgment training and it is not unusual for a scenario to include a counter-stereotype. But it is reasonable to ask whether law enforcement agencies provide *enough* of this scenario training to in-service officers to produce the effect that both theory and preliminary research says is possible. According to research by Morrison and Garner (2011), fewer than half of police agencies have access to video-simulator training and, of those that *do* have access, the level of exposure to scenarios for in-service officers (versus recruits) is very low. Six in ten of the agencies that currently have these resources expose their officers to fewer than four scenarios annually, while a quarter expose their officers to just one scenario a year. And those scenarios to which these officers are exposed may not contain the requisite elements to produce the desired outcome.

Vehicle Stop Data Collection to Measure Biased Policing

As shared above, there are a number of elements associated with the comprehensive program to produce fair and impartial policing (e.g., leadership and culture, recruitment and hiring, policy, supervision). The previous section highlighted the importance of agency training for producing bias-free policing; the measurement element is highlighted here since traffic enforcement has been key to some of the efforts to *measure* biased policing. Many agencies and several states have implemented vehicle stop data collection, whereby officers making stops record/transmit information on the stop, such as the perceived demographics of the person stopped, the reason for the stop, activities during the stop (e.g., search), the disposition of the stop (e.g., ticket) and so forth. There are benefits and costs of vehicle stop data collection (see Fridell 2004, 2017). On the "pro" side, data collection can convey the agency's commitment to unbiased policing, can give the agency information on what officers are doing, and might deter biased policing. On the other hand, the cons or costs include the time it takes officers to fill out forms and for supervisors to ensure they are being submitted, the resources devoted to data input and analysis, and the misuse or misreporting of results. And much of the debate, too, is centered on this question: *what can we actually measure?* The aspiration, of course, is to measure biased policing and yet these systems are wanting relevant to that goal. What agencies or their social science partners can do with these data is measure disparity. For instance, the data can be used to determine if, for instance, one demographic group is stopped disproportionate to its representation in a comparison (benchmark) population. What is much more challenging, however, is determining the causes or sources of disparity. The identified disparity might be produced in part by law enforcement bias, but it could also be produced in whole or in part by other legitimate factors such as differences in driving quantity, quality and location (see Fridell, 2004). The fact that disparity is not to be equated with police bias is often lost on key audiences, including community members and the press.

Agencies that choose to engage in vehicle stop data collection, or that are required to, would be well served to partner with a social scientist for designing the system and conducting the analysis. (And, remember, many university professors will offer their services without charge, in exchange for the use of the data in their research.) Agencies should also involve key community stakeholders in the discussion and planning early on and educate these individuals on the promise and constraints associated with data collection so that they can assist agency leaders in conveying the true meaning of the results to the broader public.

But also important is maintaining perspective with regard to where vehicle stop data collection fits into an agency's commitment to bias-free policing. Data collection imperfectly measures biased policing; all of the other elements of a comprehensive program (outlined above) actually do something about it. Therefore, it is legitimate for an agency leader with finite resources to decide that measurement is not as important as effective implicit-bias awareness training, use-of-force video training with exposure to counter-stereotypes, or other efforts designed to produce bias-free policing.

22 To be most effective, research on implicit bias indicates that these scenarios with counter stereotypes should be placed in ambiguous-threat situations. See Fridell 2017.

Conclusion

Concerns on the part of community members of biased policing go way back in our history. For many years, leaders were frustrated in their attempts to understand and respond to these concerns. Fortunately, the social scientists have provided important information that can advance our understanding of, and our efforts to achieve, biased policing. Police professionals—from the line level to the corner office–have new tools to promote bias-free policing in traffic enforcement and all other law enforcement activities.

Notes:

1. Amodio, D.M. & Mendoza, S.A. (2010). Implicit intergroup bias: Cognitive, affective, and motivational underpinnings," in *Handbook of implicit social cognition*, eds. Gawronski, B. & Payne, K., New York, NY: Guilford Press, 253–274.
2. Blair, I.V., Ma, J.E., & Lenton, A.P. (2001). Imagining stereotypes away: The moderation of implicit stereotypes through mental imagery. *Journal of Personality and Social Psychology*, 5(81), 828 – 841.
3. Correll, J., Park, B., Judd, C.M., & Wittenbrink, B. (2002). The police officer's dilemma: Using ethnicity to disambiguate potentially threatening individuals. *Journal of Personality and Social Psychology*, 86(6), 1314 – 1329.
4. Correll, J., Park, B., Judd, C.M., Wittenbrink, B., Sadler, M.S., & Keesee, T. (2007). Across the thin blue line: Police officers and racial bias in the decision to shoot. *Journal of Personality and Social Psychology,* 92(6), 1006–1023.
5. Dasgupta, N. (2004). Implicit ingroup favoritism, outgroup favoritism and their behavioral manifestations. *Social Justice Research,* 17 (2), 143–169.
6. Dasgupta, N. & Rivera, L.M. (2008). When social context matters: The influence of long-term contact and short-term exposure to admired, outgroup members on implicit attitudes and behavioral intentions. *Social Cognition*, 26(1), 112 – 123.
7. Dovidio, J.F., Kawakami, K. & Gaertner, S.L. (2002). Implicit and explicit prejudice and interracial interaction. *Journal of Personality and Social Psychology,* 82(1), 62–68.
8. Dovidio, J.F., Kawakami, K., Johnson, C., Johnson, B., & Howard, A. (1997). On the nature of prejudice: Automatic and controlled processes. *Journal of Experimental Social Psychology,* 33, 510–540.
9. Dovidio, J.F., Kawakami, K., Smoak, N., & Gaertner, S.L. (2009). The nature of contemporary racial prejudice. In Petty, R.E., Fazio, R.H. & Brinol, P. (Eds.), *Attitudes: Insights from the new implicit measures*, NY, New York: Taylor & Francis Group, 165–192.
10. Fridell, Lorie A. (2004). *By the numbers: A guide for analyzing race data from vehicle stops.* Washington, DC: Police Executive Research Forum.
11. Fridell, Lorie A. (2017). *Producing bias-free policing: A science-based approach.* Springer International Publishing.
12. Greenwald, A.G. & Krieger, L.H. (2006). Implicit bias: Scientific foundations, *California Law Review,* 94(4), 945–967.
13. Kubrin, C.E. & Weitzer, R. (2003). Retaliatory homicide: Concentrated disadvantage and neighborhood culture. *Social Problems*, 50(2), 157 – 180.
14. McNulty, T.L. & Bellair, P.E. (2003). Explaining racial and ethnic differences in adolescent violence: Structural disadvantage, family well-being, and social capital. *Justice Quarterly*, 20(1), 1 – 31.
15. Meehan, A.J. & Ponder, M.C. (2002). Race and place: The ecology of racial profiling African American motorists. *Justice Quarterly*, 19(3), 399 - 430.
16. Morrison, G.B. & Garner, T.K. (2011). Latitude in deadly force training: Progress or problem? *Police Practice and Research*, 12(4), 341 – 361.
17. New York State Task Force on Police-on-Police Shootings (2010). Reducing inherent danger: Report of the task force on police-on-police shootings. Unpublished report retrieved on 3/20/2017 from http://samuelwalker.net/wp-content/uploads/2010/07/Police-on-Police_Shootings.pdf
18. Fridell, Lorie A. (2017). *Producing bias-free policing: A science-based approach.* Springer International Publishing.
19. Lynch, M.J., & Michalowski, R.J. (2006). *Primer in radical criminology.* Fourth edition. Monsey, MY: Criminal Justice Press.
20. Nier, J.A. (2005). How dissociated are implicit and explicit racial attitudes? A bogus pipeline approach. *Group Processes & Intergroup Relations*, 8(1), 39–52.
21. Patterson, K., Grenny, J., McMillan, R., & Switzler, A. (2012). *Crucial conversations: Tools for talking when stakes are high.* Second Edition. New York, NY: McGraw Hill Professional.
22. Petty, R.E., Fazio, R.H., & Brinol, P. (2009). The new implicit measures: An overview, in Petty, R.E., Fazio, R.H. & Brinol, P. (Eds.), *Attitudes: Insights from the new implicit measures*, NY, New York: Taylor & Francis Group, 3–18.
23. Plant, A.E., Peruche, M.B., & Butz, D.A. (2005). Eliminating automatic racial bias: Making race non-diagnostic for responses to criminal suspects. *Journal of Experimental Social Psychology*, 41(2), 141 – 156.
24. Plant, A.E. & Peruche, M.B. (2005). The consequences of race for police officers' responses to criminal suspects. *Psychological Science*, 16(3), 180 – 183.
25. Sampson, R.J., Morenoff, J.D., & Raudenbush, S. (2005). Social anatomy of racial and ethnic disparities in violence. *American Journal of Public Health*, 95(2), 224 – 232.
26. Tyler, Tom R., and Huo, Yeun J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts.* New York: Russell-Sage Foundation.

Author:

Lorie Fridell is a former Director of Research at the Police Executive Research Forum and currently on faculty in the Department of Criminology at the University of South Florida. She is a national expert on biased policing and creator of the Fair & Impartial Policing training program (www.fairandimpartialpolicing.com).

Highly Automated and Connected Vehicles



By: **Staff Sergeant Terence McDonnell,** New York State Police, Albany, New York

Technology advancements are transforming society on a daily basis and this is especially true of automotive transportation. The modern motor vehicle is a computer-controlled machine that is becoming increasingly automated. Fully self-driving vehicles, once a thing of fantasy, are today considered inevitable. While this transformation may be unnerving to some, it holds tremendous potential to reduce motor vehicle crashes and their resultant injuries and fatalities. The National Highway Traffic Safety Administration (NHTSA) estimates that human error is a factor in more than 90 percent of traffic crashes. Therefore, if human operation is removed from the driving task, tremendous public safety benefits should be attainable. In addition, the integration of technologies that allow modern motor vehicles to continually communicate both with each other and with the roadway infrastructure promises to improve safety and efficiency and thereby improve public health. Finally, driverless cars promise increased mobility and independence for large segments of society, including the elderly, the blind, and the physically and mentally challenged.

However, such transformative technologies do not come without risk, and regulators and lawmakers are challenged

to strike a balance between encouraging testing and deployment of these vehicles on public roads and potentially hampering technological development due to perceived safety threats. States and political jurisdictions worldwide have taken varying approaches in this regard.

At the federal level in the United States, NHTSA issued its first Federal Automated Vehicles Policy in September 2016, which the Secretary of Transportation acknowledged was not intended to be the final word but merely a framework and foundation on which to build for the future. [1] Indeed, the NHTSA Policy is not regulatory in nature, serving merely as guidance to the industry. It is important to realize that such technologies are also applicable to commercial motor vehicles and there is a tremendous potential for improved safety and economy for connected and automated trucks. Like NHTSA, the Federal Motor Carrier Safety Administration (FMCSA), which bears responsibility for the safety of the nation's trucking industry, is also engaged in an ongoing effort to balance its safety mission without hampering technological development and integration in the trucking industry.

Autonomous Vehicles: Revolution or Evolution

The history of vehicle automation has largely followed two divergent strategies: a revolutionary approach and an evolutionary one. The revolutionary approach is dedicated solely to the development of fully autonomous vehicles, based largely on GPS tracking, integrated mapping and telemetry, and development of artificial intelligence to enable the vehicle to "recognize" its environment and "learn" how to respond appropriately based upon millions of miles of experience, much the same way humans learn to drive. The evolutionary approach is based upon integration of multiple technologies and capabilities, such as lane centering, crash avoidance, blind spot monitoring, and adaptive cruise control, which may allow a human operator to cede driving responsibilities to the vehicle itself under certain circumstances only, enroute to perfection of the systems and ultimately to autonomous driving.

SAE International (formerly the Society of Automotive Engineers) developed a six level taxonomy for automated vehicles ranging from no automation (Level 0) to full automation (Level 5) in order to provide a standard framework for the industry and regulators alike [2]. This system has been widely adopted and includes a lexicon of standard terms used in the industry. Highly automated vehicles are considered Levels 3 and 4, and are differentiated by whether the human operator needs to be prepared to take control of the vehicle under circumstances outside of the vehicle's operational design capabilities (Level 3 – Conditional Driving Automation) or if the vehicle itself is capable of achieving a minimal risk condition without human intervention under such circumstances (Level 4 – High Driving Automation). A Level 5 vehicle is fully autonomous and may be designed to operate without manual steering or operational controls or even without a human onboard.

Connected Vehicles

In contrast to autonomous vehicle technology, connected vehicle technologies refer to any of a variety of communications technologies which facilitate information sharing between vehicles (vehicle-to-vehicle, also known as V2V), between vehicles and the roadway infrastructure (vehicle-to-infrastructure, also known as V2I), and the vehicle and anything (V2X), including via the internet and "cloud-based" applications. Connected vehicle technologies are largely envisioned to operate on a Dedicated Short Range Communications (DSRC) frequency (5.9 GHz) set aside by the Federal Communications Commission (FCC) specifically for this purpose. DSRC technologies are capable of V2V communications up to about 300 meters, and V2I with roadside equipment at a range of 800 meters or more [3]. Other communications technologies, such as 4G and 5G, may also be integrated in connected vehicles. A wide variety of V2X capabilities are possible, including:

- Intersection and vehicle-to-vehicle collision avoidance
- Intersection control for traffic volume harmonization
- Approaching emergency vehicle warnings
- Roadway alerts and traveler information
- Vehicle performance optimization and resultant fuel economy/environmental benefits
- Commercial vehicle safety inspection clearance
- Toll and parking management.

Several connected vehicle technologies are under development specifically for use by the law enforcement/ first responder community, including:

- Intersection signal prioritization for emergency vehicles
- Enhanced interoperability between first responders enroute to or on the scene of emergencies
- Situational awareness and staging guidance
- Public messaging to approaching traffic from on scene first responders
- Public messaging to aid "move over" law compliance
- Automatic notifications to dispatch points

- Direct communications with highly automated or fully autonomous vehicles
- Electronic VIN and vehicle pedigree transmission to emergency responders to identify potential hazards at crash scenes prior to approach.
- Although connected vehicle technologies have evolved relatively independent of autonomous vehicle technologies, there are obvious safety benefits of integrating both to achieve a safety synergy.

Law Enforcement Concerns

While highly automated vehicles hold great promise for the improvement of public safety, there are also significant law enforcement concerns inherent in the testing and deployment of these vehicles on public roads, particularly as they integrate with traditional vehicles under human operation. These include, but are not limited to:

- Enforcement of traffic laws, operator responsibility, and liability
- Risks to first responders from unintended movements/ unexpected behavior
- Access to data for crash investigations
- Vehicle response to manual traffic controls/hand gestures
- Vehicle response to emergency vehicles
- Vehicle identification as highly automated or fully autonomous vehicles
- Cybersecurity and criminal use
- Criminal behavior targeting vehicles with predictable behavior
- Commercial vehicle safety and integration of automated commercial vehicles with traffic
- Training needs of law enforcement officers nationwide

Technological advancements are occurring rapidly. Although industry and safety organizations alike caution against the temptation to enact laws and regulations governing highly automated vehicles, law enforcement should stay informed and engaged on the issues. It is incumbent upon law enforcement leaders to ensure that the needs and concerns of their officers and communities are given proper consideration as jurisdictions consider the testing and subsequent deployment of highly automated and connected vehicles.

Notes

1. "Federal Automated Vehicles Policy," *National Highway Traffic Safety Administration*, page 6, September 2016.
2. "Taxonomy and Definitions of Terms Related to Driving Automation Systems for On-Road Motor Vehicles," *SAE International*, J3016, January 2014, revised 2016-09, http://standards.sae.org/j3016_201609/.
3. Connected Responder Business Needs Case Framework, Rylex Public Safety Consulting, 2016

Legalization of Marijuana: Issues for Traffic Safety



By: **Dr. Darrin T. Grondel,** *Director*, Washington Traffic Safety Commission and *Chairman*, Governor Highway Safety Administration

Throughout the U.S., marijuana is the most commonly detected non-alcohol drug found in drivers who died within one hour of a motor vehicle crash. Data from the National Highway Traffic Safety Administration (NHTSA) National Roadside Survey (NRS) in 2013-2014, noted that more than 22.5 percent of night-time drivers tested positive for illegal, prescription, or over-the-counter medications (based on the combined results of either or both oral fluid and blood tests. [1, 2, 3] Additionally, 8.6 percent of weekend nighttime drivers tested positive for psychoactive THC. This number increased to 12.6 percent in the 2013- 2014 NRS, a 48 percent increase. [4]

In 2012, Washington State and Colorado were the first states to legalize recreational marijuana. This set the stage for numerous state public initiatives and legislative actions around the U.S., resulting in a patchwork of differing marijuana laws.

As a result, law enforcement executives are grappling with the various challenges legalization poses to the safety of their communities, especially in the arena of fatal and serious injury collisions due to drug impaired driving. This article provides a high-level overview of lessons learned, areas of focus, resources and training, and other useful information to enhance a jurisdictions preparation, response, and resource allocation.

Marijuana 101

This basic overview is critical in establishing a foundation for understanding the definitions and terminology prior to jumping into a discussion of marijuana legalization. Law enforcement professionals are generally attuned to marijuana and its impairing effects, however, what do we really know about cannabis? Do we understand the chemistry and the differences between delta-*9tetrahydrocannabinol (Δ9-THC), 11-Hydroxy-THC or 11-OH-*

THC and *11-nor-9-Carboxy THC or THC-COOH*, known as Carboxy and why this is important?

"Marijuana or cannabis consists of 483 compounds and 84 different cannabinoids - these are different classes of chemical compounds that act on cannabinoid receptors in cells that repress neurotransmitter release in the brain." [5] In examining the various THC metabolites, it is important to understand the differences between psychoactive (impairing) and inactive (not impairing). The following is not a scientific resource but for contextual purposes only:

THC or delta-9tetrahydrocannabinol (Δ9-THC) is the most well-known cannabinoid and the main psychoactive substance found in marijuana.

Hydroxy-THC *11-Hydroxy-THC or 11-OH-THC*, is a psychoactive metabolite of THC formed in the body after marijuana is ingested or consumed.

Carboxy-THC is an inactive metabolite of THC formed in the body after marijuana is consumed and is not a psychoactive substance. Carboxy-THC can remain in the body for days or weeks and may show up in chemical tests, indicative of recent use. Carboxy-THC is not a useful indicator for impairment.

Marijuana is significantly different than alcohol; however, the public and even some within the criminal justice community erroneously try to compare them, especially when it comes to per se blood concentrations. Per se relates to a statutory prohibition of a blood concentration. For example, 5 Nanograms/mLis used by some states as a cutoff, whereby anyone over 5 nanongrams/mL is presumed to be impaired. The chemical composition, methods of ingestion, absorption, and presentation of impairment between marijuana and alcohol are very different. The patch work of legislation and the lack of research have resulted in three types of per se laws for driving under the influence of drugs:

- Per se: illegal to drive with amounts of specified drugs in the body exceeding set statutory limits. The Per Se limits in the United States range from zero tolerance to 5 nanograms.
- Driving Under the Influence of Drugs (DUID): illegal to drive while impaired by any drug or substance.
- Zero Tolerance: illegal to drive with any amount of specified drugs in the body.

See NMS (2014) for key provisions of each state's laws and procedures.

There are a number of research studies regarding the effects of THC on the brain, including evidence that THC binds with cannabinoid receptors in the brain, the hippocampus (short-term memory), cerebellum (coordination), and basal ganglia (area of the brain managing unconscious muscle movement), and other parts of the body. Marijuana is a lipid (fat) soluble, and is therefore stored in the fatty tissues (including the brain), as opposed to water-soluble, like alcohol, which distributes into areas of the body with a high water content, such as the blood. [6]

The legalization movement has raised the awareness of the importance of enforcement and toxicology. Officers traditionally make a stop on a suspected impaired driver, make observations of the driver's behavior, notice the presence or lack of an odor of intoxicants, conduct standard field sobriety tests (SFST) and make an arrest based on the totality of the circumstances. In many cases, once a breath alcohol reading in excess of .08g is obtained, the officer generally concludes the investigation without considering if drugs might also be a consideration of impairment. Unfortunately, legalization has identified this gap in the DUI investigation process. Toxicology reports are indicating the presence of multiple drugs to include alcohol in a driver's system, also known as poly drug use, which could be amplifying the impairment but is not being collected as part of the DUI investigation. Officers also need to be conscientious of drivers who exhibit signs of impairment and have a low portable breath test (PBT) or BAC result. It is not uncommon for those who have consumed drugs to have also consumed a beer or two prior to driving and, if stopped, would produce a low PBT reading and potentially be released without further investigation.

Despite the increased risk of drugged driving, jurisdictions are operating from a deficit in regards to baseline data, reliable database systems, and consistent data on marijuana or drug related crashes.

Data

Legalization has highlighted a significant data gap, "Most state data on drugged driving in its current form is of limited use for measuring and tracking drugged driving incidents, evaluating the effects of changing laws... and or improving our knowledge about drug use and driving impairment." [7] Inadequate data systems at a national, state, and local level are complicating the issues and providing a misperception to the public regarding the level of risk resulting from drugged driving. Law enforcement leaders need to play an active role in current and future database systems, weighing in on the type of data collected, and methods of collection, with consideration of improving the quality and value of the data.

In Washington state, an evaluation of crash reports and toxicology highlighted the importance of delineating

between the presence of active or non-active THC and other drugs and impairment. The increase in testing puts additional pressures on labs by requiring more trained technicians, supplies, and hours in court.

Fatal and serious injury crash reports may display the quantity of a drug listed, but may only indicate one drug even though the toxicology report identified several substances in the drivers system. The NHTSA Fatality Analysis Reporting System (FARS) captures alcohol use and the BAC level; however, FARS only allows for three drugs to be entered into the fatality report, by name only and does not allow for the blood level. FARS is the official database for all fatality crashes in the United States and should have no limitations on the number of substances entered and should include the toxicology results for a national perspective on drugs involved in fatality crashes.

A question that states with legalized marijuana often receive is, "Have fatality collisions increased with drivers positive for THC?" This is a difficult question to answer with the lack of good baseline data. In response to legalization, Washington state completed a descriptive report entitled, "Driver Toxicology Testing and the Involvement of Marijuana in Fatal Crashes, 2010-2014." The analysis on fatality crashes delineated psychoactive THC and non-active Carboxy-THC, to assess potential impacts of legalization on fatality crashes. In 2014, 84.3 percent of Washington drivers positive for cannabinoids were positive for active THC, compared to only 44.4 percent of cannabinoid-positive drivers in 2010. In this descriptive report, of 75 drivers involved in fatal crashes who tested positive for active THC, approximately half (38) exceeded the 5 ng/ml THC per se limit. In 2015, 36.4 percent of fatalities involved a drug-positive driver and 19.9 percent involved an alcohol-impaired driver, marking the fourth year in a row where drug involvement occurred more frequently than alcohol impairment. Many drivers were impaired by a combination of multiple drugs or by drugs and alcohol, an increasingly-common factor known as the "poly-drug use." Washington drivers involved in fatal crashes who were under the influence of multiple drugs (including alcohol) rose from 82 in 2011 to 146 in 2015, a 78 percent increase. In Washington State from 2013 - 2015, impaired drivers (including those with alcohol BAC >= .08 or drug-positive) were a factor in nearly half (49.4 percent) of all traffic fatalities and 19.2 percent of all serious injuries. Impaired driver-involved fatalities increased 6.5 percent in 2013 - 2015 (717) compared with 2010 - 2012 (673). [8]

Law enforcement leaders must consider data collection, methods, and sources as one of their highest priorities in addressing drugged driving, regardless of whether their jurisdiction is facing legalization or not. This data is essential to accurately and objectively educate the public and future jurors on the issues of drugged driving.

Public Perception

Several state and national surveys have identified a divergence in public perceptions between drunk driving and drugged driving. The results demonstrate a public indifference towards drugged driving (Responsibility.org) and abhorrence to drunk driving. The public tend to view drunk driving as clearly dangerous and socially unacceptable with decades of research to substantiate the dangers of alcohol-impaired drivers. Conversely, with mixed information and a lack of substantive research regarding drugged driving, the public does not feel strongly one way or the other about drugged driving. As a result of legalization and the fervent debate surrounding impairment by marijuana, leading researchers from around the world are undertaking a variety of research proposals to better understand the science of marijuana impairment.

Law enforcement organizations working collaboratively with their respective stakeholders need to develop key messaging using accurate data and relevant research to show the impacts of marijuana use on impaired driving.

The Pacific Institute for Research and Evaluation (PIRE), on contract with the National Highway Traffic Safety Administration, conducted a Roadside Survey in Washington State in 2014 and 2015, where they surveyed 926 drivers in five counties. Of drivers who said they had used marijuana within two hours of driving, 67 percent said that it made no difference in their driving with some respondents indicating it made them a safer driver. This self-reported data is an area of opportunity to educate the public on what is known about marijuana and the impacts it has on the brain, overall coordination, depth perception and ability to operate a motor vehicle. [9]

Research

The overarching theme around legalization of marijuana remains a knowledge gap around the effects of cannabis (and other drugs) on driving. This is challenging for those on both sides of the issue. Some proponents of marijuana legalization claiming it is safer than alcohol, they are safer drivers, and it has no effect on driving. Over the past 40 years empirical research clearly demonstrates a strong relationship between BAC levels and levels of impairment. Conversely, research establishing levels of impairment with psychoactive drugs is not well documented. Research in this area is challenged since, "Most psychoactive drugs are chemically complex molecules, whose absorption, action and elimination from the body are difficult to predict, and considerable differences exist between individuals with regard to the rates with which these processes occur." [10] The strength and potency of marijuana has changed dramatically, especially since legalization. While most governmental research involving marijuana utilized THC

levels of 3-6 percent, this is well below what states are seeing in the varying products available to consumers (flower, edibles, liquids, and other consumable products), which have been recorded with THC levels closer to 30-40 percent and hash oils reaching upwards of 92 percent THC. The impact these products have on driving requires additional research to accurately reflect crash risk.

Enforcement

Drug impaired driving may be perceived as being more complex than alcohol-impaired driving, necessitating officers to have a higher level of training and expertise. However, drug impaired driving should not be seen as more challenging. The officers do need to have some additional training to identify the signs and symptoms to successfully determine drug impairment. In some states SFST training is not part of the basic Police Officer Standards and Training certification course, which should be included and mandated for all officers.

Law enforcement leaders need to ensure their officers are SFST trained and maintain certification if applicable in their jurisdiction. Agencies should also consider training all officers in Advanced Roadside Impaired Driving Enforcement Training (ARIDE), and in consideration of agency size and geographical dispersion should have a number of officers trained as Drug Recognition Experts (DREs).

Due to the complexity and time required to process a drug-impaired driver and challenges in prosecution, law enforcement leaders need to be aware of the issues to be actively engaged in helping officers stay motivated in combatting overall impaired drivers.

Jurisdictional Considerations

The preceding information provided a foundation of the issues and challenges with legalization relevant for law enforcement leaders. The following are considerations for executives to consider in addressing the issue of legalization and the impacts on impaired driving.

- Creation of an Impaired Driving Task Force or Working Group comprised of various disciplines and subject matter experts. Some states have included a representative from the marijuana industry. The group can outline the roles, responsibilities, and deliverables but should consider:
  - Developing baseline data if possible with current data available and identifying the gaps
    - » Crash – arrest data, toxicology, hospital, public perceptions/attitudes on driving, healthy youth surveys, etc.
  - Assess
    - » Current DUI and DUID laws – definitions, laws, gap analysis
    - » Medical and Recreational – what is truly medical? What conditions? Dosage? How is it managed? Who will regulate?
    - » Judicial – review current laws, sanctions, and training – comparison with legalized states and countries
    - » Impaired driving training in respective jurisdictions
- Develop and implement an educational campaign with materials in multiple languages and relevant to various cultures
- Evaluate data collection sources (e.g. traffic crash data, toxicology, poison control, hospital, etc.)
  - What information is collected? How is it collected? Who has access for analysis? Are the systems connected for data sharing to get a broader perspective?
- Creation of a Marijuana Regulatory Agency
  - Full enforcement authority
  - Track from seed to sale
  - Packaging requirements with THC level, not attractive to children
  - Rules and regulations
- Seek dedicated funding sources from marijuana revenues for education and enforcement
- What DUID laws will be considered:
  - Illegal to drive while impaired by any drug or substance or,
  - Zero Tolerance – Illegal to drive with any amount of specified drugs in the body or,
  - Per se: illegal to drive with amounts of specified drugs in the body exceeding set limits
- Law enforcement training to include SFTS, ARIDE, and DRE
- Utilize Traffic Safety Resource Prosecutors to support prosecution and training
- Process of developing or enhancing electronic search warrants for blood

- Chemical Evidence – Oral Swabs, Blood or Urine
  - Phlebotomy for LE officers – this is a paradigm shift and provides support for the system of arrest creating efficiency with more timely evidence collection, single chain of custody for blood evidence and testimony, and can be done road side or at a secure facility.
  - What percentage of surviving and deceased drivers are tested for drugs in your jurisdiction? Do the coroners or medical examiners provide a toxicology screen with the death certificate?
- Toxicology evidence collection and analysis – How will it be collected? What are the screening tolerances? What impacts will legalization have on the crime lab and what resources are needed? Is the lab centralized or do samples need to go out of state?

The legalization of marijuana highlights new and unique challenges for law enforcement organizations, the criminal justice system, and our communities. The local, state, and national data on impaired driving, particularly drugged driving, is on the rise and compelling to take action. Throughout the U.S., we are seeing significant changes in our culture and social acceptance of impairing drugs, as such law enforcement executives need to prioritize traffic safety training, initiatives, and programs to combat impaired driving. This needs to be a collaborative approach to addressing key processes and countermeasures to support public safety and the quality of life in your community.

This chapter has provided you with a deeper understanding of the issues and challenges of marijuana legalization, including lessons learned from states that have legalized. Law enforcement executives should assess each jurisdictional consideration, in particular the training their officers have received and available training to elevate their skills, which should be a foundational step moving forward.

Notes:

1. Berning, A., Compton, R., & Wochinger, K. (2015). Results of the 2013–2014
2. National Roadside Survey of alcohol and drug use by drivers. (Traffic Safety Facts Research Note. Report No. DOT HS 812 118). Washington, DC: National Highway Traffic Safety Administration.
3. Ramirez, A., Berning, A., Carr, K., Scherer, M., Lacey, J. H., Kelley-Baker, T., & Fisher, D. A. (2016). Marijuana, other drugs, and alcohol use by drivers in Washington State (Report No. DOT HS 812 299). Washington, DC: National Highway Traffic Safety Administration.
4. http://www.nhtsa.gov/staticfiles/nti/pdf/812299-WashingtonStatedrugstudy.pdf
5. Washington Traffic Safety Commission (2015). Driver Toxicology Testing and the Involvement of Marijuana in Fatal Crashes, 2010-2014 http://wtsc.wa.gov/wp-content/uploads/dlm_uploads/2015/10/Driver-Toxicology-Testing-and-the-Involvement-of-Marijuana-in-Fatal-Crashes_REVFeb2016.pdf
6. Ramirez, A., Berning, A., Carr, K., Scherer, M., Lacey, J. H., Kelley-Baker, T., & Fisher, D. A. (2016). Marijuana, other drugs, and alcohol use by drivers in Washington State (Report No. DOT HS 812 299). Washington, DC: National Highway Traffic Safety Administration.
7. http://www.nhtsa.gov/staticfiles/nti/pdf/812299-WashingtonStatedrugstudy.pdf
8. Ibid. Ramirez, Berning, Carr, Scherer, Lacey, Kelley-Baker, & Fisher, 2016, p. 27.
9. National Institute on Drug Abuse. "What is Marijuana?" https://www.drugabuse.gov/publications/drugfacts/marijuana (accessed July 14, 2017).
10. Arnold, L. S., & Scopatz, R.A. (2016). Advancing drugged driving data at the state level:
11. Lindsay S. Arnold & Robert A. Scopatz, "Advancing Drugged Driving Data at the State Level: Synthesis of Barriers and Expert Panel Recommendations," AAA Foundation (March 2016). https://aaafoundation.org/wp-content/uploads/2017/12/AdvancingDruggedDrivingData.pdf.

Resources:

Arnold, L. S., & Scopatz, R.A. (2016). Advancing drugged driving data at the state level: Synthesis of barriers and expert panel recommendations. Washington DC: AAA Foundation. Retrieved from https://aaafoundation.org/advancing-drugged-driving-data-at-the-state-level-synthesis-of-barriers-and-expert-panel-recommendations/

Arnold, L. S. & Tefft, B.C. (2016) Driving Under the Influence of Alcohol and Marijuana: Beliefs and Behaviors, United States, 2013 – 2015. Washington DC: AAA Foundation. Retrieved from https://www.aaafoundation.org/driving-under-influence-alcohol-and-marijuana-beliefs-and-behaviors-united-states-2013-2015.

Banta-Green, C., Rowhani-Rahbar, A., Ebel, B.E., Andris, L.M., & Qiu, Q. (2016). Cannabis Used Among Drivers Suspected of Driving Under the Influence or Involved in Collisions: Analysis of Washington State Patrol Data. https://www.aaafoundation.org/cannabis-use-among-drivers-suspected-driving-under-influence-or-involved-collisions-analysis

Berning, A., Compton, R., & Wochinger, K. (2015). Results of the 2013–2014 National Roadside Survey of alcohol and drug use by drivers. (Traffic Safety Facts Research Note. Report No. DOT HS 812 118). Washington, DC: National Highway Traffic Safety Administration.

Governors Highway Safety Association. (2014). Drug Impaired Driving: What States Can Do Now. Retrieved from http://ghsa.org/html/publications/2015drugged.html

Logan, B., Kacinko, S.L, Beirness, D.J. (2016). An Evaluation of Data from Drivers Arrested for Driving Under the Influence in Relation to Per Se Limits for Cannabis. Washington DC: AAA Foundation. https://www.aaafoundation.org/evaluation-data-drivers-arrested-driving-under-influence-relation-se-limits-cannabis

NMS (2014). Stop DUID (2014): A State-by-State Analysis of Laws Dealing with Driving Under the Influence of Drugs. Willow Grove, AP: NMS Labs. stopduid.org/report.html.

Pacific Institute of Research and Evaluation (2014).

Washington State Roadside Survey, October 2014. Calverton, MD: Pacific Institute for Research & Evaluation.

Ramirez, A., Berning, A., Carr, K., Scherer, M., Lacey, J. H., Kelley-Baker, T., & Fisher, D. A. (2016). Marijuana, other drugs, and alcohol use by drivers in Washington State (Report No. DOT HS 812 299). Washington, DC: National Highway Traffic Safety Administration. http://www.nhtsa.gov/staticfiles/nti/pdf/812299-WashingtonStatedrugstudy.pdf

Ramirez, A., Berning, A., Carr, K., Scherer, M., Lacey, J. H., Kelley-Baker, T., & Fisher, D. A. (2016). Marijuana, other drugs, and alcohol use by drivers in Washington State (Report No. DOT HS 812 299). Washington, DC: National Highway Traffic Safety Administration.

Repp, K.K. and A.L. Raich (2014). Marijuana and health: A comprehensive review of 20 years of research. *Washington County Health and Human Services*. Hillsboro, OR: Washington County.

Tefft, B.C., Arnold, L. S., & Grabowski, J.G. (2016). Prevalence of Marijuana Involvement in Fatal Crashes: Washington State, 2010 – 2014. Washington DC: AAA Foundation. https://www.aaafoundation.org/prevalence-marijuana-use-among-drivers-fatal-crashes-washington-2010-2014

Van Elsland, P. & Fournier, J., & Jaffard, M. (2012). Influence of cannabis on fatal traffic crash: A detailed analysis. Transportation Research Record, pp.43-50.

Washington Traffic Safety Commission (2015). Driver Toxicology Testing and the Involvement of Marijuana in Fatal Crashes, 2010-2014 http://wtsc.wa.gov/wp-content/uploads/dlm_uploads/2015/10/Driver-Toxicology-Testing-and-the-Involvement-of-Marijuana-in-Fatal-Crashes_REVFeb2016.pdf

Are Red Light Cameras an Effective Crash-Reduction Solution?

By: **Richard J. Ashton,** *Chief of Police (Retired),* Frederick, Maryland

Picture a young family leaving a large suburban shopping mall in a late model SUV after an afternoon of shopping for summer clothes for an upcoming vacation and enjoying pizza and ice cream. As their SUV enters the roadway from the mall on a green traffic signal and begins to make a left turn, it is broadsided by a pickup truck that fails to stop for a red traffic signal. The family members' lives are shattered forever. Even though all were using appropriate occupant restraints at the time of the crash, the 29-year-old father is pronounced dead on the scene; the 6-year-old son sustains serious internal injuries; and his 4-year-old sister and his mother suffer no physical injuries. The 26-year-old driver of the truck is uninjured.

Sadly, this scenario was repeated, on average, more than twice a day in the United States in 2008 when 762 lives were lost in crashes resulting from red light violations. [1] Sixty-four percent of those killed in 2009 were in vehicles other than the one that ran the red light. [2]

When traffic control signals operate as intended, they facilitate the systematic movement of the greatest amount of traffic in the least amount of time with the greatest amount of safety and with the least amount of congestion. However, when drivers fail to heed signals' directions, crashes often occur, and, sometimes, our relatives, neighbors, friends, and coworkers are seriously injured or killed. In 2005 and 2006, about 21 percent of all traffic fatalities in the United States occurred at intersections, and approximately 30 percent of those intersections were signalized. [3]

Law enforcement officers initiate effective enforcement actions—ideally on the days and at the times and locations that these violations historically have transpired—to increase red light compliance and thereby reduce the needless deaths and injuries they produce. Realistically, however, officers are unable to undertake traffic enforcement as often as they wish because of competing demands and ever-growing workloads at a time when their agencies' authorized strengths and budgets are dwindling. Even when officers are able to enforce against red light violations, their efforts often add to existing congestion and lead to frustration when these officers cannot safely apprehend violators or even stop their vehicles on shoulders that are sufficiently wide.

Automated red light photo enforcement cameras (red light cameras) "can prevent the most serious crashes" [4] and can augment—not supplant—officers' enforcement efforts. These programs have grown exponentially in the United States, from 1 in 1992 [5] to 535 in April 2011; [6] have been supported by the IACP since 1998; [7] and should serve only one purpose: to enforce 24/7 against red light violations in an effort to reduce the crashes they trigger, as well as the deaths and injuries they cause.

Following are several items that support the effectiveness of red light cameras: [8]

- A 2011 study compared fatal intersection crash rates before (1992–1996) and after (2004–2008) 14 U.S. cities with populations of 200,000 or more had implemented red light cameras and then compared those results to 48 similarly sized cities without cameras during both periods. It found that the average annual rate of fatal red light–running crashes had

declined for both study groups, but the decline had been greater for cities with red light cameras than for cities without them (35 percent versus 14 percent); and that the average annual rate of all fatal crashes at signalized intersections had decreased by 14 percent for cities with red light cameras and had increased slightly (2 percent) for cities without them. The study concluded that red light cameras had reduced the citywide rate of fatal red light–running crashes and, to a lesser but still significant extent, the rate of all fatal crashes at signalized intersections. [9]

- Howard County, Maryland, began testing red light cameras in 1994; has utilized them for enforcement since 1997; has regularly evaluated its program; and has found "substantial overall crash reductions at almost every approach that had a red light camera," with the majority of the approaches experiencing reductions in excess of 10 percent. [10] Overall, Howard County realized a 31 percent reduction in all crashes, a 42 percent decrease in angle crashes, and a 30 percent decline in rear-end crashes. [11] Moreover, a 2002 socioeconomic cost of collision study conducted by the Maryland State Highway Administration at Howard County and other Maryland red light camera sites identified statistically significant reductions in overall crashes and in left-turn crashes, which resulted in an average cost savings of $196,000 per intersection studied. [12]
- When the Virginia legislature allowed the statute under which red light cameras had been authorized to lapse in 2005, the relative risk of red light running in the months immediately following their discontinuation was 2.63 times higher at four Virginia Beach intersections, and it increased at those same intersections to 3.59 times higher one year after the law's demise. [13]
- A study conducted between July 1, 2007, and June 30, 2008, by the Texas A&M University System's Texas Transportation Institute of 56 intersections with red light cameras in 10 Texas cities showed an average 30 percent decrease in overall crashes, as well as an average 43 percent reduction in right-angle crashes. [14]
- The Transportation Research Board's 2003 synthesis suggested that "automated enforcement of red light running can be an effective safety countermeasure." [15]To that end,
    - *There is a preponderance of evidence, albeit not conclusive, indicating that red light–running camera systems improve the overall safety of intersections where they are used . . . There is also evidence, also not conclusive, that there is a "spillover" effect to other signalized intersections within a jurisdiction.* [16] *Although nearly every study and crash analysis performed . . . has had some experimental design or analysis flaw or deficiency, there is considerable "evidence" that [red light] cameras do have an overall positive effect.* [17]

Considerations

While evidence supports the effectiveness of red light cameras, jurisdictions considering their use should think about several issues to ensure program success.

- Red light cameras should be implemented only to benefit public safety and once an engineering study supporting their installation at the intersection or intersections under consideration has been completed. Unfortunately, too many jurisdictions have obtained red light cameras to generate revenue by placing them at intersections through which many drivers run red lights but that lack histories of serious collisions amenable to reduction via red light cameras. Some exacerbate this situation by reducing the length of the yellow change interval at the same time as the cameras became operational, obviously creating additional violations and more revenue to offset budget shortfalls or to fund other items. One small municipality even attempted to fund from red light camera fines a police officer retirement system. However, this municipality failed to realize that the jurisdiction's limited number of red light cameras working 24/7 would achieve only its goal of significantly reducing violations and would not produce a meaningful revenue stream over time.
- Jurisdictions considering the installation of red light cameras need to investigate first what is causing the crashes they wish to reduce. Not all collisions at red light–controlled intersections can be cured by red light cameras. A poorly designed intersection or a signal obscured by sunlight at certain times will not become safer with red light cameras. Philadelphia, Pennsylvania, mixed and matched its solution by increasing the yellow change interval by about one second, reducing red light violations by 36 percent [18] and, by installing several months later red light cameras, decreasing red light violations further by 96 percent. [19] Other jurisdictions have achieved success simply by increasing the yellow change interval, which the Federal Highway Administration (FHWA) recommends be a minimum duration of three seconds and a maximum duration of six seconds. [20]



Source: National Cooperative Highway Research Program

- A conscientious review of the photographs taken by red light cameras should be undertaken before any action against an alleged violator is initiated. This process ensures that anything other than bona fide violations are eliminated early on; should be conducted by experienced law enforcement officers, who could be retirees or officers assigned to limited duties; and prevents the embarrassment of citing a violator whose vehicle did not commit a clear-cut violation, was in a funeral procession, or whose registration plate was obscured. Only about 35 percent of photographs in Sacramento, California, result in the issuance of citations. [21]

- One of the reasons for installing traffic control signals is to reduce the frequency and the severity of certain types of crashes, especially right-angle collisions. [22] Of the approximately 21 percent of traffic fatalities in the United States occurring at intersections in both 2005 and 2006, about 46 percent of them were T-bone collisions and only 5 percent were rear-end crashes. [23] Broadside crashes have declined in many jurisdictions where red light cameras have been adopted. For example, Oxnard, California, realized a 32 percent decrease in T-bone crashes and a 68 percent reduction in right-angle collisions involving injuries. [24] Although some studies have indicated that the installation of red light cameras has increased the number of rear-end crashes, others have not. [25] In any event, rear-end crashes tend to be less serious in terms of injury and cost than right-angle crashes. [26] Perhaps rear-end crashes will decline once motorists become acclimated to vehicles' stopping at yellow lights rather than continuing through intersections—the latter of which many did prior to the installation of cameras. In the aforementioned Texas study of 56 intersections, rear-end collisions increased 5 percent (by 5 crashes) during the 12-month study; however, in terms of those occurring at intersections where there had been more than 10 crashes per year, the number of rear-end crashes actually decreased. [27] In the Oxnard study, rear-end crashes increased a statistically insignificant 3 percent. [28] In Howard County, they dropped a total of 30 percent at all but one involved site. [29]

- Red light cameras are a relatively new enforcement technology, and their adoption may require amending existing laws or ordinances so a jurisdiction's program is not derailed when reality conflicts with prevailing statutes. Consulting with competent legal counsel; contacting nearby jurisdictions to ascertain what legislative obstacles they have encountered; and reviewing such publications as the FHWA and the National Highway Traffic Safety Administration's *Red Light Camera Systems Operational Guidelines*, [30] the IACP's *Highway Safety Desk Book*, [31] and the IACP's *Manual of Police Traffic Services Policies and Procedures* [32] during the program's planning phase will allow jurisdictions to identify and avoid the pitfalls others endured.

Final Thoughts

Red light camera programs should be evaluated periodically to recognize whether or not their intended purpose still is being achieved. The importance of discovering intersections where crashes are not declining is as significant as identifying those where they are, so the former can be analyzed further to ensure the appropriate crash-reducer is implemented. The results of these evaluations may yield information upon which to focus future efforts. For example, the study of 46,997 red light violations at 11 intersections in Sacramento, California, between May 1999 and June 2003 [33] suggested that as the age of the violator increased, the probability of running a red light while speeding decreased; [34] that most violations occurred during the daytime, with the highest frequency being between 2:00 p.m. and 2:59 p.m.; [35] that about 56 percent of the violating vehicles were not speeding at the time of violation; [36] that more than 94 percent of red light violations occurred within two seconds after the onset of the red light; [37] and that about 4 percent of the violators were repeat offenders. [38] Releasing to the public findings such as these contributes to the transparency of the program.

Perhaps if red light camera citations were accompanied by points against violators' driver's licenses rather than by fines akin to parking citations, the cameras would reduce even more the frequency of crashes and the needless injuries and deaths they cause. Granted, the number of citations issued would decrease in response to the threat of points, and more citations would be challenged before

the judiciary because the consequences of sustained violations would be greater. However, the controversy relative to revenue generation might finally be divorced from the public safety purpose on which the adoption of red light cameras should be based. The current tendency is to regard a violation linked to a vehicle's owner rather than to its driver as a mere inconvenience, and this perception would be eliminated.

The success of red light cameras can be linked to the program's transparency. If the public safety purpose of red light cameras, as well as the operation of the program, is discussed extensively in various forums throughout the jurisdiction prior to implementation; if appropriate signage is provided to apprise drivers of the use of red light cameras; if reports of malfunctioning cameras are investigated promptly and, when verified, incorrect citations are rescinded; and, if a straightforward means of contesting what drivers believe are improperly issued citations is provided and publicized, many negative issues can be avoided and public support for the effort can be garnered. A jurisdiction that operates by itself as much of the red light camera program as it is able generally will gain greater public acceptance of it. For example, while Texas allows a jurisdiction to contract for certain aspects of a red light camera program, it prohibits a jurisdiction from "agree[ing] to pay the contractor a specified percentage of, or dollar amount from, each civil penalty collected." [39] The manner in which contractors have been compensated has been in many jurisdictions as contentious an issue as the creation of cash cows.

While red light cameras are not a panacea, their judicious use can achieve what law enforcement officers cannot: 24/7 enforcement against red light violations and a resulting decline in lives needlessly lost and in serious injuries sustained.

Notes:

1. "Red Light Running," Federal Highway Administration (FHWA) Safety.
2. Wen Hu, Anne T. McCartt, and Eric R. Teoh, *Effects of Red Light Camera Enforcement on Fatal Crashes in Large US Cities* (Arlington, Va.: Insurance Institute for Highway Safety, February 2011), 2.
3. "2005 vs. 2006 Intersection Fatality Comparison," FWHA Safety.
4. Hu, McCartt, and Teoh, *Effects of Red Light Camera Enforcement on Fatal Crashes in Large US Cities*, 10.
5. National Cooperative Highway Research Program, *NCHRP Synthesis 310: Impact of Red Light Camera Enforcement on Crash Experience* (Washington, D.C.: Transportation Research Board, 2003), 3.
6. "Communities Using Red Light and/or Speed Cameras," Insurance Institute for Highway Safety, Highway Loss Data Institute.
7. Highway Safety Committee, "Red Light Camera Systems Operational Guidelines," IACP Resolution adopted at the 112th Annual Conference of the International Association of Chiefs of Police (Miami, Florida, 2005); and Highway Safety Committee, "Support for Automated Enforcement Technologies," IACP Resolution adopted at the 109th Annual Conference of the International Association of Chiefs of Police (Minneapolis, Minnesota, 2002).
8. National Campaign to Stop Red Light Running, "Get the Facts about Photo Enforcement," table Red Light Camera Results in Specific U.S. Cities.
9. Hu, McCartt, and Teoh, *Effects of Red Light Camera Enforcement on Fatal Crashes in Large US Cities*, 1.
10. Glenn Hansen, "Utilization and Impacts of Automated Traffic Enforcement," statement before the U.S. House of Representatives Committee on Transportation and Infrastructure, June 30, 2010, 4.
11. National Cooperative Highway Research Program, *NCHRP Synthesis* 310, 24.
12. Hansen, "Utilization and Impacts of Automated Traffic Enforcement," 4.
13. Bryan E. Porter, Kristie L. Hebert Martinez, and Johnnie F. Bland, *Survive the Drive Coalition* research, abstract, Old Dominion University, January 16, 200.
14. Troy D. Walden, *Analysis on the Effectiveness of Photographic Traffic Signal Enforcement Systems in Texas* (Crash Analysis Program of the Center for Transportation Safety, Texas Transportation Institute, Texas A&M University System, November 2008), 21.
15. National Cooperative Highway Research Program, *NCHRP Synthesis* 310, 2.
16. Ibid.
17. Ibid, 38–39.
18. Richard A. Retting, Susan A. Ferguson, and Charles M. Farmer, *Reducing Red Light Running through Longer Yellow Signal Timing and Red Light Camera Enforcement: Results of a Field Investigation* (Arlington,Va.: Insurance Institute for Highway Safety, January 2007), 1.
19. Ibid.
20. FHWA, "Highway Traffic Signals," chap. 4 in *Manual on Uniform Traffic Control Devices for Streets and Highways*, 2009 ed., 489.
21. C.Y. David Yang and Wassim G. Najm, *Analysis of Red Light Violation Data Collected from Intersections Equipped with Red Light Photo Enforcement Cameras*, March 2006, DOT HS 810 580, 11.
22. FHWA, "Highway Traffic Signals," 434.
23. "2005 vs. 2006 Intersection Fatality Comparison," FWHA Safety.
24. Hu, McCartt, and Teoh, *Effects of Red Light Camera Enforcement on Fatal Crashes in Large US Cities*, 2.
25. Ibid, 3.
26. Ibid.
27. Walden, *Analysis on the Effectiveness of Photographic Traffic Signal Enforcement Systems in Texas*, 31.
28. National Cooperative Highway Research Program, *NCHRP Synthesis* 310, 11.
29. Ibid, 24.
30. FHWA and National Highway Traffic Safety Administration, *Red Light Camera Systems Operational Guidelines*, January 2005, FHWA-SA-05-002, 14, 37–52.
31. IACP Highway Safety Committee, "Use of Automated Enforcement," in *Highway Safety Desk Book* (Alexandria, Va.: September 2004), 112–21.
32. IACP Highway Safety Committee, "1.28 Photo Enforcement," in *Manual of Police Traffic Services Policies and Procedures* (Alexandria, Va.: July 2004), 80–81.
33. Yang and Najm, *Analysis of Red Light Violation Data Collected from Intersections Equipped with Red Light Photo Enforcement Cameras*, 11.
34. Ibid, 39.
35. Ibid.
36. Ibid, 19.
37. Ibid, 35.
38. Ibid, 25.
39. Photographic Traffic Signal Enforcement System, Texas Transportation Code § 707.003(b

Speed Cameras to Reduce Speeding Traffic and Road Traffic Injuries

By: **Rebecca Steinbach, Chloe Perkins, Phil Edwards, Deirdre Beecher, Ian Roberts**

Background

Exceeding the speed limit is one of the most common criminal offenses committed in the United Kingdom and can engender tremendous social harm. Speed limits on roads regulate traffic speeds by establishing a safe upper limit on vehicle speeds. Consequences of exceeding the speed limit can be severe with a direct relationship between speeding vehicles and increased crash risk. Many countries have seen an increase in the use of automatic speed enforcement to enforce traffic speed limits, detect speeding vehicles and reduce road traffic collisions and injuries that result from them. These methods employ speed detection devices such as cameras, which may be monitored or unmonitored, mobile or fixed, overt or covert. Speed cameras mostly use speed sensors to trigger a camera to capture an image of any vehicle (and its number plate) travelling above a pre-set speed. Modern systems use digital and video cameras and are able to transmit information over data networks. Once the evidence has been reviewed and an offence verified, a notification is sent to the registered owner of the vehicle. Sanctions for committing an offence can include licence points, driving bans, fines and driver awareness courses. The focus of this review is on the use of all types of speed cameras to prevent speeding, road traffic collisions and injuries and fatalities resulting from road traffic collisions.

Objectives

The aim of this review was to update and expand a Cochrane systematic review of traffic speed enforcement cameras, and to explore under which circumstances speed cameras may, or may not work, and to assess whether any effects differ by type of device (i.e. covert versus overt, fixed versus mobile cameras). The update included studies published after 2010 (the date of the last Cochrane update) and has been expanded by including information on mechanisms, moderators, implementation and economic costs of speed camera interventions (EMMIE framework). [1]

Search methods

We searched the following electronic databases: OVID Transport database (1988 to June 2015); National Police Library (to June 2015), Cochrane Injuries Group Specialised Register (to 16/03/2015), Cochrane Library CENTRAL database (to 16/03/2015); Ovid MEDLINE(R), Ovid MEDLINE(R) In-Process & Other Non-Indexed Citations, Ovid MEDLINE(R) Daily and Ovid OLDMEDLINE(R) (1946 to 16th March 2015); Embase Classic+Embase (OvidSP) (1947 to 16th March 2015); ISI WOS: SCI-EXPANDED (1970) & CPCI-S (1990) to 16th March 2015); PROQUEST (to 12/06/2015); EBSCO (to 12/06/2015); Web of Knowledge (to 12/06/2015); Heritage (to 12/06/2015).

Selection criteria

Randomised controlled trials, interrupted time series and controlled before-after studies that assessed the impact of speed cameras on traffic speeding, road crashes, crashes causing injury or fatalities, were eligible for inclusion.

Data collection and analysis

We independently screened studies for inclusion, extracted data from full text reports, and assessed methodological quality. We reported study authors' outcomes and calculated standardised results based on the information available in each study.

Results

The systematic review is based on a total of 51 primary studies including the 35 studies in the previous Cochrane review and an additional 16 evaluations uncovered from our searching which met the selection criteria. Nine of the primary studies in the review were carried out in the UK, 11 from Australia, five from the USA. The remaining studies were carried out across a number of other countries (including Denmark, Finland, Germany, Spain, Hong Kong, Belgium, South Korea, Netherlands, New Zealand, Canada, Norway, and Italy).

The evidence evaluated in this updated review shows speed cameras bring about consistent reductions in both speed and collision outcomes. Results suggest that the implementation of speed camera programmes is associated with a:

- 7 percent reduction in average speed
- 52 percent reduction of vehicles exceeding the speed limit
- 19 percent reduction in collisions
- 18 percent reduction in collisions resulting in injuries
- 21 percent reduction in severe or fatal collisions.

There was no evidence that the effect of speed cameras differed by whether the camera was overt or covert. However, there was some evidence to suggest that fixed cameras had a slightly greater effect on all road traffic collisions and those resulting in fatalities or severe injuries, than mobile cameras.

Authors' conclusions

This review was sufficiently systematic that most forms of bias that could influence the study conclusions could be ruled out and provides evidence that speed cameras are an effective intervention for reducing speeding behaviour, and can help combat some of the negative consequences of speeding such as fatalities and injury collisions. Considering continuing increases in traffic volumes, speed cameras appear to be a worthwhile intervention to protect public safety.

Notes:

1. Johnson, S.D., Tilley, N. & Bowers, K.J. 2015. "Introducing EMMIE: An evidence rating scale to encourage mixed-method crime prevention synthesis reviews." *Journal of Experimental Criminology* 11, 459-473. https://doi.org/10.1007/s11292-015-9238-7

Unmanned Aerial Systems and Traffic Safety



By: **Brad Blair,** *(ret.) Deputy Commissioner,* Ontario Provincial Police

The Ontario Provincial Police (OPP), Traffic Safety and Operational Support Command have been operating Unmanned Aerial Systems (UAS) since 2012. This technology is utilized to enhance our search and rescue capabilities, for forensic Identification purposes, as well as collision scene mapping as part of the *Rapid Clearance* mandate within the Highway Safety Division (HSD).

The UAS compliments, but does not replace, the OPP's aviation assets. The current OPP UAS provides imagery through high resolution digital video, still images and Forward Looking Infrared Cameras (FLIR). The small size and autonomy allow these UAS units to reach areas that may be too treacherous or difficult for officers to be deployed. The resilience that these units have to snow, rain, and wind provide search managers with continued, low maintenance aerial assets available at all times. It also allows for aerial photography and 3D modeling of complex crime scenes.

The OPP was one of the first police services in Ontario to utilize a UAS for major collision investigation. In 2013, the Traffic Support Unit – HSD deployed two units in the Greater Toronto Region. The UAS utilizes aerial photography and video to create an ortho-mosaic aerial image of a collision scene. The aerial images provide officers the ability to capture the objective collection of scene evidence in significantly less time and replaces the traditional Robotic Total Station for mapping at collision scenes. The UAS has a proven ability to provide a faster investigative process through a photo "grid-map". On average, the Traffic Support Unit – HSD maps a major collision scene in twenty-two minutes.

The UAS software also provides the Reconstructionist better analysis tools to review and animate a collision scene. The UAS software is capable of creating 2-D and 3-D images of a scene. The scene images can be manipulated to allow for various vantage points within the collision. Images can be linked together to allow for a visual representation moving through the collision scene, for example, a vehicle path of travel. Accuracy of all the UAS images is within one centimeter per pixel and similar to traditional scene mapping tools. The more technologically advanced UAS images and visual representations provide invaluable representations of the collision scene to both to the Reconstructionist and court when applicable. The UAS directly contributes to rapid clearance while extending investigative excellence at major collision scenes.

As the technology advances and the regulations are set in place to guide both private and commercial use of these small aerial units, the technological advantages and cost savings that will be realized will certainly be substantial and their use amongst police services will likely expand significantly.

5 Ways NG911 Can Improve Your Agency

Adapted from NG911 Next Generation 911 for Leaders in Law Enforcement. An educational supplement produced in coordination with the International Association of Chiefs of Police, the National Sheriffs' Association and 911.gov. 2013.

Improved Officer Safety

With NG911, a 911 "call" will take very different forms: Staff at PSAPs will be able to receive, process and store text, pictures and videos from citizens. Even better, that information can be quickly — sometimes almost immediately — relayed to first responders, giving them more precise information. For example, access to live video from cameras inside a bank being robbed could give responding officers valuable information about suspects, weapons and the number of hostages.

NG911 also permits other digital information, such as maps, to be forwarded to officers, says Marcoux. "Most of the law officers [in Vermont] have mobile data terminals in their vehicles so we could push a map out to them instead of having the 911 operator relay this information verbally," he explains. "When you're working alone in a rural situation, the more information the officer has, the safer he will be." Dispatchers could quickly send backup to help a wounded

officer wherever he is in a sprawling rural area. Another benefit will be the ease in which dispatchers can share intelligence with officers, providing additional information on what could be a dangerous situation.

In the future, the effectiveness of the NG911 system's ability to share data back and forth with officers in the field should increase as the First Responder Network Authority (FirstNet) establishes a wireless public safety broadband network.

Improved Efficiency

One big benefit of NG911: The new technology will allow PSAPs to identify the location of callers — especially those on wireless devices — faster and more accurately so law enforcement can find citizens quickly in an emergency. "Because NG911 provides more precise location information automatically, an officer won't spend as much time looking for a car that went off the road and into a ditch," says Mark Grady, founder of INdigital Telecom which provides NG911 technology to the state of Indiana.

Getting more evidence in the form of videos and photos will be very useful when it comes to solving cases or taking them to trial. "If someone snaps a picture of a license plate or a suspect, that's obviously beneficial to law enforcement," says Marlys R. Davis, E-911 program manager for King County in Seattle.

With this information, a deputy or officer would be able to identify and catch a suspect more easily. Adds Chief Reyes: "We would significantly increase the apprehension and case-closure rate with the amount of evidence coming into our center." Transferring a 911 caller's information between jurisdictions is far easier, too, when agencies are on the same Internet Protocol (IP) technology. Jackie Mines, director of emergency communication networks for the Minnesota Department of Public Safety, couldn't do that with her previous network. "That alone is a huge benefit," she says.

Improved Public Safety

In 2005, the year before NG911 came to Indiana, Grady says that a citizen who dialed 911 would wait 23 to 27 seconds for the call to be routed to a 911 operator; with NG911, that's now less than 3 seconds. "If you're waiting for someone to take a call during a domestic violence situation, things can go sideways on you pretty quick," he notes.

Texting for help is also potentially life-saving when citizens can't make a call or speak without endangering themselves. The major wireless carriers have agreed to support texting to 911 by 2014, however, NG911 texting applications will continue to improve upon the proposed services.

911.gov

Source: 911.gov

Similarly, an upgraded emergency response system will provide better public service in a natural disaster or other emergency. NG911 call centers will be able to instantly re-route a call to another tier of PSAPs if the first is not available. This was essential when Vermont was struck by Hurricane Irene. "Our second-busiest PSAP in Rutland had to be evacuated," says Jim Lipinski, former Enhanced 911 IT manager for Vermont, one of the first U.S. states with a statewide NG911 system. "In a traditional 911 system, calls would have queued up and people would have abandoned them." But during the storm and its aftermath, the system was able to distribute the load throughout Vermont – meaning every 911 call was answered swiftly.

Better Access for Special-Needs Communities

The deaf and hard-of-hearing, the mentally disabled, the physically disabled and senior citizens will especially benefit from an upgrade to the nation's 911 system, since it will be easier for them to reach 911 with their phones, without requiring additional devices. Judy Flores, director of the Black Hawk Consolidated Communications Center in Waterloo, Iowa, helped launch the country's first text-to-911 program in 2009. "The biggest benefit so far is allowing our citizens to have that extra access point, in particular our hard-of-hearing and speech-impaired community," she says. "They have the same access as anyone else [now]."

Potential Costs Savings

Upgrading to NG911 is not inexpensive, but over time, the agencies that upgrade will save money through efficiencies. Vermont was able to save significant funds by rerouting 911 calls from a PSAP that was taking less than 1 percent of the state's calls because the new IP technology can pick up calls from other parts of the state. As already noted, it's easier, faster and less expensive to share information between jurisdictions and agencies; many communities and regions will likely combine their resources to make the transition to NG911 possible.

Then there are the incalculable costs. Says Flores, "If you save one life because you made an improvement, how can you measure that?"

Public Relations and Messaging in the Digital Age



By: **Katie Nelson,** *Social Media and Public Relations Coordinator,* Mountain View Police Department

Police departments are not strangers to the need to develop solid working relationships with journalists, especially from their local media outlets. But with the advent and subsequent astronomical rise in the use of social media by the public, the ability to connect with a wider audience is no longer an elective pursuit, it is an inevitable one. And unlike in the past, when departments relied on media representatives to try and showcase or highlight a particular message from police agencies, we now have the opportunity to take total control of that story and tell it how we would like to in a digital sphere, every time. That ability to quickly and effectively connect and message is particularly important when it comes to traffic and highway safety.

Far too often, social media management and public information officer duties are part of a collateral assignment and as a result, the department spokesperson has potentially little to no experience in communicating with the media or adequately utilizing social media tools to effectively organize and champion a public relations campaign. Even more detrimental is the potential for a lack of enthusiasm behind an online campaign or a public safety message due to an insufficient understanding of what truly integral pieces public relations and social media are to an agency. There is so much opportunity to have a message that resonates through and beyond your community.

Public Information

How do you want to be viewed by those you serve? The public perception you build is almost entirely defined by how you choose to connect and converse with your audience. Nothing replaces the ability to go out and personally meet with your residents, which creates an almost immediate sense of support and confidence within your community. The more face time you can have with your business owners, neighbors, and schools, the greater opportunity you have to define your agency's brand – the public display of the mission statement your department personnel work to personify every day.

Such an effort should also not be limited to just the public relations role. This should be an exercise that is accomplished regularly from the top down. The more who buy in and understand and support the need to regularly connect with the community, either through in-person programs or social media campaigns, the greater the likelihood will be that your agency builds a brand that is considered transparent and trustworthy.

While some agencies will have the opportunity to develop a role dedicated solely to social media management and public relations, others could potentially have a team implemented for these efforts. Some departments are unable to do either, but that in no way hinders an agency's ability to have a solid public information outreach program.

Both external and internal information are key functions of a public relations role, and communicating capably under each of these is imperative to the vitality of the department's didactic enterprises, particularly when it comes to efforts around traffic safety messaging.

To note, information dissemination differs greatly for each. External outreach – most effectively done through social media channels for most agencies — informs and educates the public of department business with regards to department efforts and activities. It gives your residents a chance to ask questions, and be informed of actions taken on behalf of the department. It also allows the media to cover it if they so wish, but your need for them is greatly diminished by your agency's own ability to provide the information yourselves, in essence making you a primary source of information, and the local media, secondary. It also allows you to message at opportune times throughout the day. By doing so, you increase the chance that your message is not only read, but understood, shared and discussed. This once again bolsters your efforts made to regularly enhance the overall department image.

Internal public information is disseminated to department employees for the purpose of providing information on internal activities and on employee achievements. Always have a way for your personnel to see how the public is reacting to external messaging. Department morale often benefits from the positive notations made, particularly on social media, of a job well done for which officers are rarely thanked for in person and in public.

Social Media

Social media is one of the most effective and relevant ways to communicate with your residents, especially if done correctly.

Studies have shown that roughly 79 percent of online adults (roughly 68 percent of all U.S. adults) use Facebook. [1] That is more than triple the number of online Americans who use Twitter (24 percent) or Instagram (32 percent). [2] In addition, a social media mobile exclusive app that cannot be ignored is Snapchat, where an average of more than 10 billion videos are shared a day. [3] Nextdoor, a hyperlocal social media site, is also coming of age in a social sphere where a majority of internet users are digital natives.

Other websites such as YouTube and LinkedIn continue to share space in the ever-expanding social media realm, but they do not possess the juggernaut messaging opportunities that sites like Facebook do.

Agencies should, at this point, be well established in their presence on most of these platforms, depending on their community's specific use, and experimenting regularly with messaging efforts to gauge what the public prefers to see and read.

But what many agencies are still failing to accomplish are effective messaging strategies on platforms that not only encourage engagement, they are increasingly demanding it.

> *For successful engagement, understand that social media is the language and digital platforms are dialects. Fluency in both matters.*
>
> – Captain Chris Hsiung, *Mountain View Police Department*

Today, social media platforms should not be utilized to merely blast information to the public. Rather, they should be considered places where agencies and the residents alike can converse and engage. Two-way engagement is critical in building trust and transparency with the public as well as creating effective social listening options for agencies to understand their communities and what their communities are discussing both online and off. [4]

Two-way engagement has been statistically proven to be an asset to agencies. Captain Zach Perron of the Palo Alto, California, Police Department definitely proved this in "Beyond the Digital Bullhorn: The Benefits of Two-Way Engagement Strategy."

The study was conducted over several months. It conclusively proved that the more an agency actively responded to inquiries and commentary on social media platforms, the agency not only attracted more followers – a benefit to spreading critical information when needed by your department – it also suggested that an agency would be viewed more favorably and as being more willing to be more "transparent" than those who did not utilize this communication tactic. [5]

Such efforts can directly correspond to traffic safety messaging. The public is far more willing to appreciate notifications on traffic alerts, enforcement efforts, and educational opportunities if you 1) communicate to them in their preferred space – online and 2) if you show a concerted effort to engage with them. Your message dies with you if you are not sharable online.

For example: an agency planning on conducting enforcement targeted specifically at speeding vehicles in school zones can capitalize on photos of officers looking out for children as they cross the street to their school. A clever reminder on social media that you are out protecting the youngest citizens in your area will overwhelmingly elicit positive feedback and responses versus zero notifications at all. To not alert residents that you will be conducting some type of traffic enforcement, for example, often leads to speculation and can result in rumors and false information being spread. It also denies you a great opportunity to positively showcase your department.

Social media truly allows you to take control of your narrative, particularly on a topic that at times can be divisive. Utilization of digital messaging allows you to get your message across to not only your residents, but to a much wider audience. It also gives you more power to effectively resonate and relate to your community that will help build much-needed trust and support over time.

Media Relations

Media relations is no longer the *most* important tool at your disposal in your quest for a good public affairs program, but it is still an *important* one. The majority of the public should have the ability to directly have contact with you through various social media channels, be it Facebook, Twitter, Nextdoor, Instagram, or Snapchat. But even with all of these free communication tools at our fingertips, nearly 90 percent of messages (these can be comments, questions, direct messages, etc.) are ignored by "brands." [6] A brand is essentially a name, symbol, or design that identifies and differentiates a product from other products. [7]

As such, this can mean that those who are feeling ignored will turn to media personnel to try and have them get the answers they seek. On average, people who pose a question on Twitter, for example, expect a response within 60 minutes. [8]

Perceptions of police have also been strongly influenced by portrayals on television, in movies, or in books. But remember, every opportunity for positive publicity can create positive opinions, but conversely, one negative experience can destroy every effort you have made to encourage your public to trust and confide in you. And more often than not, your residents include media professionals who witness your behavior both as a private citizen and as a public personality.

"Antagonistic relationships between the police and the traditional media need to become a relic of the past." – Captain Zachary Perron, *Palo Alto Police Department*.

Fear of close contact with the media, either because of an incident in which your agency received unfair treatment,

or as a result of a "horror story" from a fellow officer, are debilitating to your public relations efforts. By cutting off contact or refusing to meet with reporters – who rotate so quickly now from role to role at their respective outlets – you jeopardize your ability to not only have that news outlet's followers, viewers, or readers at your disposal for eyes and ears when it comes to your messaging campaigns, but you also risk creating a greater amount of work for your agency when it comes to establishing and maintaining public trust. The more you shy away from interacting with the press, the more likely they are to report on your agency in a biased manner or ignore you completely.

Because of the continuing decline of the journalism industry, reporters are often pulled in a multitude of directions, attempting to cover several stories in the span of a day. They often have less than eight hours to cover a story, so it can be difficult to contact them or get to know them in a greater capacity than just their byline. The quickest way to combat that is to follow them on social media. Most major news outlets now require their reporters to be on Twitter, for example. Follow them, and interact with them online. Invite them to your events, and suggest meeting in person in a neutral space, such as a coffee shop in your town.

While you can't change how past interactions dictated a reporter's relationship with someone in your department, your proactive efforts to engage with them can often identify a potential problem and manage its outcome. Make every effort to maintain a dialogue with media personnel in your public relations role, because the more reachable you are and the more relatable you are, your department's messaging efforts will become a higher priority for them to cover and subsequently, your message will reach potentially millions more.

Community Programs

Community programs are formal services that serve a demonstrated need within a particular community or area. They are sponsored totally or partially by the law enforcement agency and are aimed at mitigating a particular problem, or at advising a segment of the population about a specific program. These activities can include both crime prevention programs and traffic safety projects. Examples are Neighborhood Watch, Operation Identification, DARE, rape and assault prevention, child molestation prevention, bicycle safety programs, Halloween safety, departmental appearances, tours, speaking presentations, and ride-along programs.

All can be documented and promoted on social media in an effort to enhance the public's awareness of efforts your department or agency is undertaking. They can simultaneously serve as a marketing tool for your agency to showcase and highlight your officers and the multifaceted approach they take with their jobs.

Working with the Media

In your role as a public information officer, you must recognize and understand the needs and requirements of journalists and in turn, work to help them try to understand the methods, policies, and constraints under which law enforcement personnel operate. By doing so, you increase the likelihood that journalists will give you a fair opportunity to have your voice heard in their stories and even more so, that the best possible image of the department can be conveyed to the public.

News happens around the clock, and as such, it oftentimes can impact your agency, either directly or indirectly. Media outlets operate on a nearly 24-hour news cycle, with most television, radio and newspaper reporters beginning their first segments or stories of the day at 4 am and continuing well into the evening. As employment numbers in journalism continue to decline, more news organizations are being spread thinner, requiring journalists to cover several stories or topics on a given day, requiring them to become "experts" on any topic in mere hours. [9]

While different states operate under different requirements with how much information can be released on any given incident, journalists believe, and more often, so does the public, that they should report on as much detail as possible on a story they consider to be newsworthy. In this news cycle, you have minutes to jump to the front of the narrative opportunity and control the story and the dissemination of information.

When news initially breaks, something called the "newsjack" occurs. [10] The "newsjack" is a period of time where you have all the incipient, relevant information you can release, and everyone else, including the media, are scrambling for it. This period of time is vital for a public information officer. It gives them the ability to push out initial but critical information and as much safety messaging as possible, which will then in turn be shared by media professionals and public alike.

As such, this period of time is particularly vital for law enforcement agencies' use of social media. Every journalist will be looking to quickly share as much as news as possible – being first is vitally important among journalists when it comes to breaking news – and then getting ahead of the story to continue to maintain dominance. As a public information officer, you must then retain control of the narrative and storytelling as much as possible until what is known as the "archival process" – or when the story is more commonly known to be "put to bed" – is completed. Leaks will inevitably happen, and with more and more journalists using scanners as sources of information to stay ahead in the story-telling game, this can be difficult.

If an event provokes media interest, particularly on a regional, national or international scale, a story will go out, with or without your help. Law enforcement needs the media as an ally, but the media do not need us to do a story—their ability to do a story doesn't depend on us. They do, however, depend on us to keep providing timely and updated information. To fail at doing this not only sours your agency's reputation, it removes the control of the story from your hands.

Print media publications often have more space to go into finer details of a story, but they too have deadlines. Again, as the journalism industry continues to try and grapple with the ever-expanding digital sphere of available news, their deadlines have been pushed up to increasingly unreasonable times, often in the afternoon. Because of these deadlines, you can have very little time to provide information, or commentary, on a situation. Nothing looks worse for an agency than having a news source state that you either refused to comment or could not be made available for comment.

Help out journalists by not only providing relevant information, but as you update them, provide quotes and images that they can use in their stories. These can be shared oftentimes through social media in things like a livestream, or as part of an update or in a press release. The more visuals and quotes a journalist can have from your agency, the less likely they are to call you or email you to ask for them.

When you do provide comment in-person, especially for television or radio reporters, think in 10-second sound bites. You want to minimize editing by a station as much as possible, so make every word count. When you release a breakdown of a major event, do not use law enforcement jargon that could be easily bungled by someone who doesn't understand or know to what you are referring. Updates and releases that require little or no editing on a reporter's or editor's part helps minimize corrections that could potentially need to be issued if they didn't understand what was being communicated by your agency.

If you are being interviewed over the phone, which is fairly common particularly for radio stations, make sure you know you are being recorded. Only 11 states in the United States require for interviewees to be notified that they are being recorded in a phone conversation. [11] Federal law states that at least one party must be aware the phone call is being recorded for it to be legal. [12] As such, it is always acceptable to ask if you are being recorded. If you can, also take time before the official recording begins to ask what questions may be put forth by the journalist.

The same can be said for on-camera interviews. If the interview is planned, ask questions ahead of time so you know what you may need to research and so you can make sure that what you have said is accurate. When speaking with journalists in any setting, avoid as much as possible providing a personal opinion and if you realize you said something in error, rectify it.

Avoid going "off the record," either in a recorded setting or otherwise, at all costs. Also, remember that television crews also have deadlines, and are just as willing to move forward with a story, with or without you.

As the hunt for breaking news continues to rise, more televisions crews are becoming mobile and working from the field. As such, on-the-spot interviews have become commonplace for public information officers. Be sure you are trained to respond to live requests.

National News Media

Be aware that any incident in your town could potentially become regional, national, or international coverage, particularly situations such as protests or storm damage. If a traffic incident is extremely severe, that can also rouse attention of reporters out of your area. Always anticipate that the more severe an incident, the more likely it will be that you will be speaking to national media representatives.

If you are the sole public information officer for your agency, coordinate efficiently when speaking with national or international journalists. Their time zones will play a big role in their deadlines and their need to speak with you. If you have a public relations team, make sure someone is designated to speak with any journalists on-camera or on the phone is the same person who speaks with international news media. This will ensure accurate and equal sharing of information to all reporters. If your team is working together to coordinate release of information to the press, make sure the process is streamlined between those who are working on compiling information and those who are working to share it with others. This streamlining process should be practiced several times throughout the year in table-top exercises, both for teams and for sole public information officers, to make sure that when an incident does occur, you are ready and the process is as seamless as possible. As a public information officer, you should always be included in the decision-making process of what can and cannot be released.

Public Service Announcements

Public Service Announcements can be extremely effective if done in such a way that captures viewers' attention through creativity and impact. It is becoming increasingly crucial to find new and inventive ways to share the same safety announcement, be it for drunk driving, using your seatbelt or to not text and drive.

Find ways that can translate across traditional and social media channels that will resonate with your community.

Messages can be effective without always being serious; injecting humor into a PSA is oftentimes allows viewers to relate and to be entertained. It also allows them to want to listen, which should be the goal of your objective, every time.

Messages should be anywhere between 30 seconds and 60 seconds. This allows them to be played across traditional and social media platforms without any issues of needing to be trimmed down. But remember, if a viewer's attention is not captured within the first 10 seconds, they will most likely not continue to watch the remainder of the message. [13]

Managing the Media

Despite what the current climate may suggest, a majority of journalists want to provide and publish accurate information to their followers. They operate in an extremely high-stress environment, and often work long shifts and often for very low pay. To date, there are roughly 40,000 journalists employed full-time in the United States. [14] That number is expected to continue to decline as reporters seek higher paying jobs or as the burnout rate continues to intensify because of working conditions.

With these numbers declining, and with the turnover rate continuing to rise in newsrooms across the country, it is vitally important that you meet with journalists, and always exchange contact information so that the journalist knows the best way to reach you and vice versa.

If possible, instruct the journalist to follow you on social media, so that they can have access to information as quickly as possible when an incident occurs. This will relieve some of the stress on you so that you do not have to remember to individually email or call each person that requests updates on an incident.

If you must send out a news release, first make it available online on your social media channels and then send one email that encompasses all the journalists who are covering or who could potentially cover the event. It is imperative that you also have a formal department policy on handling news media, on what information can and cannot be released, and on department use of social media.

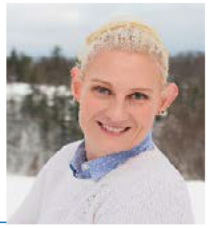
Most journalists have press credentials issued to them by their respective news agency, but if your department does issue separate credentials, let journalists know as soon as possible so that if they arrive at a scene, they will have the closest possible access without disrupting any investigations or destroying evidence.

Finally, have regular meetings – twice a year at least – to have check-ins with journalists and to make sure that any questions or concerns they may have are addressed. This will also encourage additional goodwill between your department and any media representatives.

Notes:

1. "Social Media Update 2016," Pew Research Center, accessed June 14, 2017, http://www.pewinternet.org/2016/11/11/social-media-update-2016/
2. Ibid.
3. "Snapchat by the Numbers: Stats, Demographics & Fun Facts," Omnicore, accessed June 14, 2017, https://www.omnicoreagency.com/snapchat-statistics/
4. "Mountain View Police Department's Social Media Strategy 2.0 in the Heart of Silicon Valley," California Police Chiefs Association, accessed June 14, 2017, http://www.californiapolicechiefs.org/index.php?option=com_dailyplanetblog&view=entry&year=2013&month=03&day=24&id=26:mountain-view-police-department-s-social-media-strategy-2-0-in-the-heart-of-silicon-valley
5. Becoming More Than a Digital Bullhorn: Two-Way Engagement on Twitter for Law Enforcement, Homeland Security Digital Library, accessed June 14, 2017, https://www.hsdl.org/?abstract&did=792227
6. "47 Social Media Statistics to Bookmark for 2017," Sprout Social, accessed June 14, 2017, https://sproutsocial.com/insights/social-media-statistics/
7. "Branding," Entrepreneur, accessed June 14, 2017, https://www.entrepreneur.com/encyclopedia/branding#
8. "Can you afford to lose half your customers?" Digital CX Conversations by Eptica, accessed June 14, 2017, https://www.eptica.com/blog/can-you-afford-lose-half-your-customers
9. "Employment trends in newspaper publishing and other media, 1990-2016," Bureau of Labor Statistics, accessed June 14, 2017, https://www.bls.gov/opub/ted/2016/employment-trends-in-newspaper-publishing-and-other-media-1990-2016.htm
10. "The Inbound Marketer's Complete Guide to Newsjacking," Hubspot, accessed June 14, 2017, https://blog.hubspot.com/blog/tabid/6307/bid/32983/The-Inbound-Marketer-s-Complete-Guide-to-Newsjacking.aspx#sm.0000glkzj3tu0dyvyjz1dxteywink
11. "Recording Phone Calls and Conversations," Digital Media Law Project, accessed June 14, 2017, http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations
12. "Scope of 18 U.S.C 2511 Prohibitions," Office of the United States Attorneys, accessed June 14, 2017, https://www.justice.gov/usam/criminal-resource-manual-1050-scope-18-usc-2511-prohibitions
13. "Our 8 second attention span and the future of news media," Venture Beat, accessed June 14, 2017, https://venturebeat.com/2016/12/04/our-8-second-attention-span-and-the-future-of-news-media/
14. "Occupational Employment and Wages, May 2016," Bureau of Labor Statistics, accessed June 14, 2017, https://www.bls.gov/oes/current/oes273022.htm

Traffic Incident Management (TIM)



By: **Annjanette Kremer, P.E.,** *Traffic Incident Management Engineer,* Michigan Department of Transportation

Traffic incident management (TIM) is the planned and coordinated multi-disciplinary processes used to detect, respond, and clear traffic incidents as quickly as possible while protecting the safety of on-scene responders and the traveling public. Safe, quick clearance is necessary so that traffic flow may be restored to pre-incident levels as safely and quickly as possible. An incident is defined as any non-recurring event that causes a reduction in roadway capacity. Such events include but are not limited to traffic crashes, debris in the roadway, disabled vehicles, spilled cargo, floods, and other unplanned natural or man-made events.

Given the wide range of issues involved with incidents, close coordination is required among a diverse range of traffic safety stakeholders. These stakeholders include professionals from fields that include law enforcement, fire, emergency medical services, towing and recovery, transportation, dispatch and hazardous materials, as well as the media. One of the principal concerns related to incident management is secondary crashes, which occur after the initial incident due to issues such as unexpected slowed or stopped traffic. Many times, a secondary crash is more severe than the primary crash or incident, and all incidents represent inherent dangers-to responding personnel at the scene.

Other side effects of incidents include:

- Increased response time by first responders such as emergency medical services, police, fire, towing & recovery, medical examiners, etc.

Lost time and a reduction in productivity. For each minute a freeway lane is blocked during peak use, an estimated 4 minutes of delay result after the incident is cleared accounting for 4.2 billion hours/year in delays. [1]

- Increased cost of goods and services transported by highways
- Increased fuel consumption
- Reduced air quality and other adverse environmental impacts
- Reduced quality of life for those sitting in traffic.

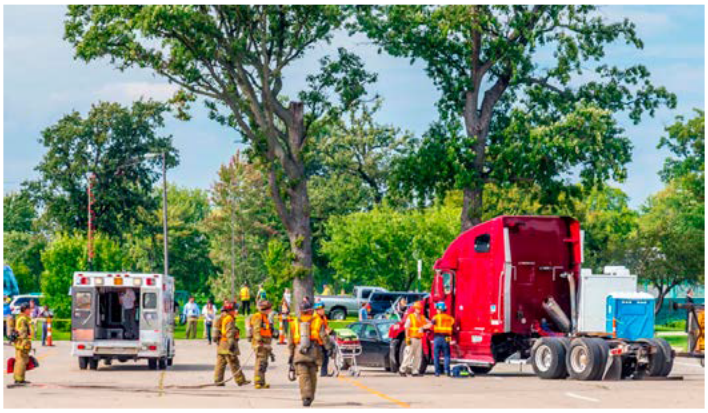


Photo credit: Michigan Department of Transportation

Prior to the development of TIM practices, traffic incidents were handled with minimal inter-agency coordination or communication. Emergency responders were dispatched to or arrived on scenes of traffic incidents to handle the duties of their specific area of expertise, including crash investigation, emergency medical services, fire services, tow and recovery, etc. What often ensued, particularly at larger scale incidents, was a chaotic response where essential responders were hampered by other responders and their parked vehicles from reaching the scene. Ambulances with injured patients could not leave the scene efficiently. TIM was developed to organize that chaos by extending the principles of the Incident Command System to the highway environment, and thereby improving coordination, efficiency, effectiveness, and safety.

Managed response means overlapping as many tasks of the many responding groups as possible without compromising the integrity of any task or safety on the scene. This can only be achieved by extensive planning involving the responding organizations, agreements on procedures and policies, and mutual program action to identify and obtain personnel and equipment resources to accomplish planned tasks.

The keys to effective traffic incident management are quick and accurate incident detection and notification; rapid response of available resources, including traffic control; safe and quick removal of the incident; effective inter-agency communications supported by integrated communications systems; and provision of accurate and reliable information to travelers in the area about the location, nature, impact, and expected duration of an incident. The components of a proper traffic incident management program include planning, detection and notification, verification and response, site management, clearance, recovery, and motorist information. Many documents on traffic incident management are available on the Internet at http://www.ops.fhwa.dot.gov/eto_tim_pse/about/tim.htm.

TIM Law and Guidance

Manual on Uniform Traffic Control Devices

Chapter 6I of the Manual on Uniform Traffic Control Devices (MUTCD) contains information on the types of temporary signs, barriers and other traffic control devices that are approved for use in traffic incident management areas. This MUTCD is available online at http://mutcd.fhwa.dot.gov/.

Laws to Promote Safe, Quick Clearance

Three general types of laws have been enacted in support of TIM

1. **Move Over:** These require drivers approaching a scene where emergency responders are present to either change lanes when possible and/or reduce vehicle speed. Move Over Laws have been enacted in every state, most Canadian Provinces, and in nations worldwide. The laws vary jurisdiction-to-jurisdiction, and law enforcement officers should be intimately familiar with the law in their jurisdiction and should be encouraged to enforce the law in earnest to improve public compliance.
2. **Driver Removal:** Also known as the "Steer It, Clear It" law, "Move It" law or "Fender Bender" law, it requires that vehicles in minor property damage crashes, be moved out of the travel lanes to a safe location where drivers can exchange information and/or wait for law enforcement assistance. By moving the vehicles from the roadway, traffic flow is restored and secondary crashes can be avoided and reduces the officer's exposure.
3. **Authority Removal:** Also known as "Hold Harmless" law, clarifies the authority and responsibility of pre-designated public agencies to clear damaged or disabled vehicles and spilled cargo from the roadway to allow normal traffic flow to resume and prevent the occurrence of secondary incidents. Authority Removal laws typically provide indemnification for these agencies if removal duties are performed in good faith and without gross negligence. [2]

The Safe, Quick Clearance Laws enhance motorist and responder safety, and reduce congestion and delay. Although a number of states, provinces and nations currently have one or more of these laws in place, observed variability in the existence, wording, and coverage of Safe, Quick Clearance Laws challenges further implementation. [3]

For more information on best practices in Safe, Quick Clearance Laws see: http://www.ops.fhwa.dot.gov/publications/fhwahop09005/quick_clear_laws.pdf.

TIM Performance Measures

Evaluation metrics provide the necessary feedback to TIM responders to allow them to improve performance. Equally important, they provide decision makers with the data to demonstrate the value of TIM activities and justify their related expenditures. The most used TIM performance measures are:

1. **Roadway clearance time:** The time between first recordable awareness of incident by a responsible agency and the first confirmation that all lanes are available for traffic flow.
2. **Incident clearance time:** The time between first recordable awareness of incident by a responsible agency and time at which the last responder has left the scene.
3. **The number of secondary crashes:** Incidents for which a response or intervention is taken, where a collision occurs either a) within the incident scene or b) within the queue (which could include opposite direction) resulting from the original incident. [4]

TIM Training and Resources

SHRP2 TIM Training

The National Traffic Incident Management (TIM) Responder Training program also known as the Strategic Highway Research Program (SHRP2) TIM Training was developed to improve the coordination of all traffic incident responders from the moment the first emergency call is made through conclusion of the incident and return of normal traffic flow.

The curriculum is based on extensive and detailed research conducted with TIM responders across the country and is based on a train-the-trainer approach. The FHWA-led 8-hour train the trainer course builds a team of instructors within each state, region, or agency. They, in turn, train their colleagues using this innovative curriculum. Shorter, four-hour courses and one-hour training modules are also available. Training modules are flexible and can be modified to fit state and local regulations or practices. A web-based training program is also available. For more information on the program or to contact the lead person in your state see: https://www.fhwa.dot.gov/goshrp2/Solutions/Reliability/L12_L32A_L32B/National_Traffic_Incident_Management_Responder_Training_Program.

TIM Network

The TIM Network is comprised of individuals representing various TIM disciplines with the goal of facilitating practical

and results-oriented communication. A key facet is continuous, specific, and relevant outreach. The goal of the TIM Network is to connect traffic incident management (TIM) professionals from across all disciplines to discuss developing issues of national interest, keep practitioners apprised of the latest industry information, and garner important input. There is no cost to join. [5]

To find more information go to http://timnetwork.org/.

Responder Safety.com

Responder Safety.com is the website of the Emergency Responder Safety Institute, which is an advisory group of public safety leaders and transportation experts committed to reducing deaths and injuries to America's emergency responders. The site is a clearinghouse of information related to TIM and first responder safety issues and includes data, news, training opportunities, PSAs, and links to other first responder organizations. [6]

Free online training, videos, and more can be found at http://www.respondersafety.com/About-Us/Default.aspx-

Notes:

1. U.S Department of Transportation, "National Support Needed to Improve Highway Safety and Reduce Congestion," http://ops.fhwa.dot.gov/publications/fhwahop12007/index.htm
2. (accessed April 21, 2017)
3. U.S Department of Transportation, "Traffic Incident Management Quick Clearance Laws: A National Review of Best Practices,"https://ops.fhwa.dot.gov/publications/fhwahop09005/quick_clear_laws.pdf (accessed April 21, 2017)
4. Ibid.
5. U.S Department of Transportation, "Performance Measures," http://www.ops.fhwa.dot.gov/eto_tim_pse/preparedness/tim/pm.htm (accessed April 21, 2017)
6. TIM Network, "About the Network," http://timnetwork.org/about-the-network/

The Incident Command System (ICS) and the National Incident Management System (NIMS)

Complex incident scenes require effective coordination of multiple resources who may bring varied training, equipment, resources, procedures and protocols. In an effort to promote standardization and more effective management of incidents, the federal government, through FEMA, has adopted the National Incident Management System (NIMS) and the Incident Command System (ICS).

According to FEMA, NIMS is a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work together seamlessly and manage incidents involving all threats and hazards—regardless of cause, size, location, or complexity—in order to reduce loss of life, property and harm to the environment. NIMS is the essential foundation to the National Preparedness System (NPS) and provides the template for the management of incidents and operations in support of all five National Planning Frameworks. [1]

ICS is a systematic tool used for the command, control and coordination of an emergency response. ICS allows agencies to work together using common terminology and operating procedures for controlling personnel, facilities, equipment and communications at a single incident scene. [2]

Federal, state and local authorities should take advantage of free training to ensure they have a clear understanding of their roles and responsibilities for successful emergency management and incident response. This can vary from the investigation of a traffic crash to managing a large scale hurricane event, such as Hurricane Harvey which impacted Texas in 2017. FEMA has made NIMS and ICS training available on the FEMA website. The Federal Highway Administration has significant information available regarding NIMS and ICS concepts and how they apply to managing traffic incidents. Law enforcement leaders are encouraged to review this information and be sure that their first responder community have been trained on these concepts. [3] Additionally, the ResponderSafety.com Learning Network provides numerous training programs including "Traffic Incident Management: Incident Command & Management" which delve into ICS concepts as they relate to a highway incident. [4]

Law Enforcement Application

NIMS and ICS is readily adaptable to law enforcement and other emergency response disciplines. Since the 1980's, law enforcement agencies have adopted the principles and continue expand the training and daily use application of NIMS and ICS in managing police emergencies.

The effectiveness of ICS training increases when an integrated approach involves regional law enforcement agencies and representatives of other emergency disciplines. This enhances closer working relationships and on-scene coordination and cooperation. Whereas perhaps in the past, training occurred more in a vacuum and was limited to law enforcement or the fire service only, now, through new partnerships, police, fire and EMS are able to train together. Enhanced communications and understanding of how ICS can work for all first responders is a key take-away of this training which can then be applied in the field. Interagency relations have been improved; and the concept of teamwork, vital to the management of complex incidents, has been established and reinforced. Response to the natural and technological disasters, civil disturbances, security and crowd control details, and the entire gamut of law enforcement activities can be managed through ICS implementation and use. ICS is a widely accepted tool among law enforcement agencies because it is logical and easy to implement yet still compatible with ICS utilized by fire and other primary emergency response disciplines. It has been accepted and

endorsed by the IACP's Highway Safety Committee as the preferred method of handling major highway emergencies.

Notes:

1. "National Incident Management System," FEMA, accessed September 1, 2017, https://www.fema.gov/national-incident-management-system
2. "Simplified Guide to the Incident Command System for Transportation Professionals," U.S. Department of Transportation, Federal Highway Administration, accessed September 1, 2017, https://ops.fhwa.dot.gov/publications/ics_guide/
3. Ibid.
4. "Traffic Incident Management: Incident Command & Management," ResponderSafety.com, accessed September 1, 2017, http://learning.respondersafety.com/Training_Programs/Traffic_Incident_Management_Incident_Command_Management.aspx

Enforcement, Engineering, Education and Evaluation

The basics of an effective traffic safety program has always involved the "three E's + 1"—enforcement, engineering, and education, along with evaluation—working in conjunction for safer roads and drivers. Today, it is recognized that it involves the "four E's, plus OER"—enforcement, engineering, education, evaluation, and other emergency responders, all working together to reduce crashes and to mitigate and manage incidents, particularly at complex crash scenes. Public safety officials, state and local engineering departments, federal and state DOTs, traffic safety advocacy groups, community groups and local citizens can collaborate on initiatives to bring solutions to identified problems.

Some crashes are caused by vehicle defects. Adopting mandated federal motor vehicle safety standards, such as safety belts, supplemental restraint systems and rollover and side impact protection, have reduced the number of injuries in traffic collisions.

NHTSA is also working to promote new vehicle technologies that will further increase the potential to reduce the number of crashes. [1] NHTSA has maintained a robust vehicle safety program. The program includes the issuance of vehicle safety standards and requires manufacturers to recall vehicles and equipment that have safety-related defects. [2] You can learn more about this important NHTSA initiative on the NHTSA website. State motor vehicle safety inspection programs help to ensure that vehicles are maintained in safe operating condition and these programs identify potential vehicle failure on highways.

Enforcement

As has been mentioned in previous chapters of this Resource Guide, enforcement is also a key component to any traffic safety programs. Targeted traffic enforcement programs by law enforcement deter unsafe drivers by causing the suspension or revocation of driver's licenses for hazardous moving violations. In addition, enforcement efforts to detect vehicle equipment violations are one step in helping to identify and remove unsafe vehicles from the road.

Education

Public information campaigns conducted by the NHTSA, the GHSA, state highway safety representatives, state and local law enforcement agencies and licensing authorities, and public traffic safety advocacy agencies, along with high school and commercial driver education programs, and driver improvement programs, help educate drivers with the traffic laws and instill in them proper driving attitudes.

Engineering

Engineering is an important consideration in any effort to enhance traffic safety. Design, construction, and maintenance of highways and traffic control devices can be instrumental in reducing collisions.

Enforcement and engineering are encouraged to work in concert with one another to promote highway safety. Law enforcement officers on patrol are able to proactively help engineers in identifying potential hazards that can either be eliminated or mitigated. By reporting obscured or nonfunctioning traffic control devices and dangerous highway conditions and by providing feed- back from citizen complaints and the study of traffic congestion problems, officers can offer important input to traffic engineers.

Engineers can work with officers by making highway improvements, such as changing speed zones; erecting new types of traffic control devices; and placing roadside objects, such as utility and sign poles and guard rails, so that out-of-control vehicles are slowed or stopped without causing injury to occupants. Engineers at state highway departments utilize data from traffic crash reports to assess and improve traffic safety problems. It is important that this collaboration between law enforcement and engineers continues so potential causal factors can be identified early and funding can be allocated for traffic safety projects. A good example of a cost-effective traffic safety improvement project was detailed in an article titled "Engineering Solutions to Enhance Traffic Safety Performance on Two-Lane Highways." [3]

Evaluation

The final E stands for evaluation. Every time you make a change or adopt a new or revised strategy, you should have in mind how you will measure the results. There are many ways to evaluate your results. Pre- and post-surveys of the attitudes of motorists or the public, pre- and post-traffic or speed surveys, pre- and post-crash statistics, comparisons of citations issued for specific periods, and interviews of officers involved in a project are but a few of the methods of evaluation that can be used.

American Association of State Highway and Transportation Officials (AASHTO)

One important organization that has played an integral role in promoting highway safety through a variety of efforts is the American Association of State Highway and Transportation Officials. Representing the highway and transportation departments in the 50 states, the District of Columbia and Puerto Rico, AASHTO's primary goal is foster "the development, operation, and maintenance of an integrated national transportation system." [4] AASTO has a Standing Committee on Highway Traffic Safety that was developed in 1976 with representatives from state DOTs, NHTSA, GHSA, FHWA, AAMVA and others who are able to bring solutions to complex traffic safety and engineering-related issues. While not having a role in enforcement per se, AASHTO provides advocacy and research while raising awareness in education, engineering and evaluation efforts.

On an annual basis through AASHTO's Safety Management Meeting, a Safety Leadership Award is awarded to a state "that has made significant improvements in safety by showing leadership in safety, strong safety partnerships and strategic planning, and innovation in safety." As an example, the 2016 Safety Leadership Award winners were the State of Minnesota and the State of Tennessee. Minnesota was recognized for developing new safety countermeasures and methods for moving toward zero, including alternative designs for intersections, warning strips in pavement and vendor contracts to install safety infrastructure treatments quickly." [5]

AASHTO is an excellent resource for law enforcement leaders. With regular meetings and opportunities to share best practices at the national and regional levels, AASHTO continues to work with federal and state DOTs, engineering officials, representatives from state, county and local law enforcement agencies, traffic safety advocates and others to support national efforts to reduce fatalities and serious injuries. Annual meetings and conferences held by organizations such as the IACP's Highway Safety Committee, NHTSA and AASHTO provide opportunities for law enforcement leaders to learn more about emerging best practices in the traffic safety discipline.

Notes:

1. "Safety Technologies," NHTSA, accessed September 1, 2017, https://www.nhtsa.gov/equipment/safety-technologies
2. "Safety Issues & Recalls," NHTSA, accessed September 1, 2017, https://www.nhtsa.gov/recalls
3. "Engineering Solutions to Enhance Traffic Safety Performance on Two-Lane Highways," Hindawi, accessed September 1, 2017, https://www.hindawi.com/journals/mpe/2015/762379/
4. "AASHTO Overview," AASHTO, accessed September 1, 2017, https://www.transportation.org/home/organization/
5. "Committee on Safety," AASHTO, accessed September 1, 2017, https://safety.transportation.org/

CHAPTER 10: LEGAL ISSUES IN TRAFFIC SAFETY

Legal Issues in Traffic Safety

By: **M. Kimberly Brown,** National Traffic Law Center, National District Attorneys Association

DISCLAIMER

This Section is intended to provide a general overview of some of the legal cases related to traffic safety but is not intended to provide legal advice. A law enforcement officer needs to understand that many state courts renounce U.S. Constitutional law claiming that their particular state constitution provides greater protections to individuals than the Federal Constitution. The cases included represent the federal rules and usually the majority rule on these issues. Do not rely on these cases until you check with your state prosecutor and/or your state Traffic Safety Resource Prosecutor. Additionally, a law enforcement officer must be familiarized with the applicable laws for his enforcement jurisdiction, strategies and tactics for detecting offenders, and the elements that must be established for a successful adjudication. Further, a law enforcement officer should be knowledgeable on the legal decisions and current trends in his own locality. Lastly, a law enforcement officer may find it helpful to review the legal section of his state DUI Detection and Standardized Field Sobriety Test course in addition to this document.

Reasonable, Articulable Suspicion vs. Probable Cause

The standard for a traffic stop requires objective justification, also known as reasonable, articulable suspicion (RAS) and is based on the totality of the circumstances. Reasonableness depends on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers.

An officer cannot pull a single driver from the stream of traffic without at least an articulable, reasonable suspicion of wrongdoing. *Delaware v. Prouse*, 440 U.S. 648 (1979).

A court must consider the totality of the circumstances (*e.g.*, the whole picture) in determining whether a reasonable suspicion exists. *United States v. Cortez*, 449 U.S 411 (1981).

If a reasonable suspicion stop lasts too long, it turns into an arrest and an arrest requires probable cause. *Florida v Royer*, 460 U.S. 491 (1983).

The standard is satisfied by some minimal level of objective justification. The officer must be able to articulate something more than an inchoate and unparticularized suspicion or hunch. The 4th Amendment requires some minimal level of objective justification for making the stop. That level is considerably less than proof of wrongdoing by a preponderance of the evidence. *U.S. v. Sokolow*, 490 U.S. 1 (1989).

For the purposes of determining whether an encounter between police and an individual constitutes a seizure for purposes of the Federal Constitution's 4th Amendment, where the encounter takes place is one factor, but it is not the only one. The "reasonable person" test--under which the appropriate inquiry, in determining whether an encounter between an individual and the police is consensual for the purposes of the 4th Amendment, is whether a reasonable person would feel free to decline the officers' requests or otherwise terminate the encounter--presupposes an innocent person. *Florida v. Bostick*, 501 U.S. 429 (1991).

Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause. Reasonable suspicion, like probable cause, is dependent upon both the content of information possessed by police and its degree of reliability. Both factors, quantity and quality, are considered in the totality of the circumstances, the whole picture, that must be taken into account when evaluating whether there is reasonable suspicion. *Alabama v. White*, 496 US 325, 110 S. Ct. 2412 (1990).

The process of making a reasonable suspicion determination allows officers to draw on their own experiences and specialized training to make inferences from and deductions about the cumulative information available to them that "might well elude an untrained person." *United States v. Arvizu*, 534 U.S. 266 (2002).

Traffic Stop - General

Not all personal intercourse between policemen and citizens involves "seizures" of persons within the meaning of the 4th Amendment; only where the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen is the inference that a "seizure" has occurred justifiable. *Terry v. Ohio*, 392 U.S. 1 (1968).

A traffic stop is a seizure of the driver even though the purpose of the stop is limited and the resulting detention is quite brief. See *Delaware v. Prouse*, 440 U.S. 648 (1979).

A driver is not "seized" simply because the police have chosen to follow his or her vehicle. In order to constitute a seizure under the 4th Amendment, there must be either the

application of physical force, however slight, or submission to an officer's show of authority to restrain a subject's liberty. While a pursuit may be a show of authority—if the defendant runs away—s/he has not submitted to the authority, and no seizure therefore has occurred. *California v. Hodari D.*, 499 U.S. 621 (1991).

NOTE: Some state courts, however, have expressly refused to adopt the holding of *Hodari D.* and, instead, rely on a totality of the circumstances standard in determining whether a person has been seized, *e.g., State v. Randolph*, 74 S.W.3d 330 (2002).

Whether or not a police officer normally stops vehicles for minor traffic violations and uses the evidence of such violations as a pretext to stop vehicles for some other purpose is immaterial, as long as articulable, reasonable suspicion of some sort of law violation is present. It is not necessary to probe into the officer's mind to further justify the stop. *Whren v. U.S.,* 517 U.S. 806 (1996).

NOTE: Some state courts, however, under their state constitutions have rejected the *Whren* rule, *e.g., State v. Ladson*, 138 Wash. 2d. 343, 979 P2d. 833 (1999).

Presence in a high crime area alone is not sufficient to justify a stop, but is one factor in the totality of the circumstances. Nervous, evasive behavior is also a pertinent factor in determining articulable, reasonable suspicion for a stop. Headlong flight on the approach of a police officer is "the consummate act of evasion" and not necessarily indicative of wrongdoing but certainly suggestive of such. *Illinois v. Wardlow*, 528 U.S. 119 (2000).

Passenger in automobile stopped by police officer held to be seized within meaning of 4th Amendment and thus allowed to challenge constitutionality of the stop. The relevant question is whether a reasonable person in defendant's position after the car was stopped would have believed himself free to terminate the encounter between the police and himself. *Bredlin v. California*, 127 S. Ct. 2400 (2007).

Traffic Stop — Length / Duration

If a reasonable suspicion stop lasts too long, it turns into an arrest and an arrest requires probable cause. *Florida v Royer*, 460 U.S. 491 (1983).

A routine traffic stop is a relatively brief encounter and is more analogous to a *Terry* stop than a formal arrest. A seizure that is justified solely by the interest in issuing a warning ticket to the driver can become unlawful if it is prolonged beyond the time reasonably required to complete that mission. *Illinois v. Caballes*, 543 U.S. 405 (2005).

An officer's inquiries into matters unrelated to the justification for the traffic stop . . . do not convert the encounter into something other than a lawful seizure, so long as those inquiries do not measurably extend the duration of the stop. *Arizona v. Johnson*, 555 U.S. 323 (2009).

A police stop exceeding the time needed to handle the matter for which the stop was made violates the United States Constitution's shield against unreasonable seizures. A seizure justified only by a police-observed traffic violation, therefore, becomes unlawful if it is prolonged beyond the time reasonably required to complete the mission of issuing a ticket for the violation. *Rodriguez v. U.S.,* 575 U.S. __, 135 S.Ct. 1609 (2015).

Traffic Stop—Ordering Driver/Passengers Out of Vehicle

An officer may order a driver out of the car as a matter of course. *Pennsylvania v. Mimms*, 434 U.S. 106 (1977).

An officer may order a passenger out of the car as a precautionary measure, without reasonable suspicion that the passenger poses a safety risk. *Maryland v. Wilson*, 519 U.S. 408 (1997).

If traffic stop is valid, police can order the driver and passengers out of the vehicle. Officer can pat down driver and/or passengers if the officer reasonably concludes that the driver and/or passenger might be armed and dangerous. Can only pat down those individuals whom the officer believes to be armed and dangerous. *Arizona v. Johnson*, 555 U.S. 323 (2009).

Traffic Stop—Questions at Traffic Stop (Miranda?)

Roadside questioning of motorist detained pursuant to routine traffic stop did not constitute "custodial interrogation" for purposes of *Miranda* rule, so that pre-arrest statements motorist made in answering such questioning were admissible against motorist. *Berkemer v. McCarty*, 468 U.S. 420 (1984).

NOTE: In other words, as part of a traffic stop, an officer may engage in a limited amount general, on-the-scene questioning without giving the *Miranda* warnings, if the subject is not yet in custody. For instance, a DUI suspect could be asked what drugs he had been taking and how much alcohol he had consumed prior to driving and prior to being arrested.

NOTE: Where a DUI driver is transported to the police station and held, he is in custody for purposes of *Miranda*. Questioning in custody requires *Miranda* warnings in misdemeanor cases. *Berkemer v. McCarty*, 468 U.S. 420 (1984).

Before custodial interrogation, defendant must be warned that he has the right to remain silent and anything he says can be used against him, and he must be told he has the right to a lawyer; he may knowingly and intelligently waive these rights. *Miranda v. Arizona*, 384 U.S. 436 (1966).

Traffic Stop—Arrest

If a reasonable suspicion stop lasts too long, it turns into an arrest and an arrest requires probable cause. *Florida v Royer*, 460 U.S. 491 (1983).

The 4th Amendment does not prohibit a warrantless arrest for a minor motor vehicle offense, such as a safety belt violation, as long as the arresting officer had probable cause for the arrest. *Atwater v. City of Lago Vista*, 532 U.S. 318 (2001).

Traffic Stop—Anonymous Tip / Citizen Informant

Informant's tip may carry "sufficient indicia of reliability" to justify an investigative stop, even though it may be insufficient to support an arrest or search warrant. For purposes of determining the validity of an investigatory stop of a person's automobile based on an anonymous caller's tip that the person is engaged in criminal activity, it is not unreasonable to conclude that (1) the independent corroboration by the police of significant aspects of the caller's predictions about some facts imparts some degree of reliability to the other allegations made by the caller, including the claim that the person is engaged in criminal activity, (2) if the anonymous tip contains a range of details relating not just to easily obtained facts and conditions existing at the time of the tip, but also to future actions of third parties ordinarily not easily predicted, someone with access to such information is likely also to have access to reliable information about the person's illegal activities, and (3) where significant aspects of the caller's predictions are verified, the caller is honest and at least well enough informed to justify the stop. *Alabama v. White*, 496 U.S. 325 (1990)

In the context of information supporting an investigatory stop, the citizen-informant category of cases is treated quite differently than those involving anonymous tips. Information from ordinary citizens who have personally observed what appears to be criminal conduct carries with it an indicia of reliability and is presumed to be reliable. *State v. Ramsey*, 129 Ohio App. 3d 409, 717 N.E. 2d 1158 (1998).

While acknowledging that an anonymous tip alone seldom demonstrates an informant's basis of knowledge or veracity, under appropriate circumstances, an anonymous tip can demonstrate sufficient indicia of reliability to provide reasonable suspicion to make an investigatory stop. *Navarette v. California,* 572 U.S. ___, 134 S. Ct. 1683 (2014).

Traffic Stop—Pretextual Stop

The temporary detention of a motorist upon probable cause to believe that he has violated the traffic laws does not violate the 4th Amendment's prohibition against unreasonable seizures, even if a reasonable officer would not have stopped the motorist absent some additional law enforcement objective. Detention of a motorist is reasonable where reasonable articulable suspicion exists that a traffic violation has occurred. *Whren v. United States*, 517 U.S. 806 (1996).

The subjective intentions of individual police officers play no role in ordinary, probable cause 4th Amendment analysis. A traffic violation arrest will not be rendered invalid by the fact that it was a mere pretext for a narcotics search. *Arkansas v. Sullivan*, 532 U.S. 769 (2001).

Traffic Stop—Flight under Suspicious Circumstances

The defendant's flight from officers in area of heavy narcotics trafficking supported reasonable suspicion that defendant was involved in criminal activity and justified stop. The individual's presence in area of expected criminal activity, standing alone, is not enough to support reasonable, particularized suspicion that the person is committing a crime, but officers are not required to ignore relevant characteristics of location in determining whether circumstances are sufficiently suspicious to warrant further investigation. *Illinois v. Wardlow*, 528 U.S. 119 (2000).

Traffic Stop—Hit and Run

Requiring a driver involved in a collision to stop at the scene and provide name and address does not violate the driver's constitutional rights. *California v. Byers*, 402 U.S. 424 (1971).

Traffic Stop—Parking

The government may create parking districts and prohibit non- residents from parking on public streets in such areas. It does not violate equal protection of the law, since classifying parkers into residents and nonresidents is a reasonable classification. *County Board of Arlington County v. Richards*, 434 U.S. 5 (1977).

Traffic Stop—Roadblocks / Sobriety Check Points

As long as law enforcement officers conduct a non-discretionary roadblock, it does not violate the 4th Amendment. How many impaired drivers are arrested is not relevant. *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990).

NOTE: Some state supreme courts, however, have ruled otherwise under their state constitutions, see *State v. Koppel and Forrest*, 127 N.H. 286, 499 A2d. 977 (1985).

A checkpoint whose primary purpose was to detect evidence of ordinary criminal wrongdoing (*e.g.*, to interdict illegal drugs) was rejected by Supreme Court because it lacked individualized suspicion and because its primary purpose was ultimately indistinguishable from the general

interest in crime control. *Indianapolis v. Edmond*, 531 U.S. 32 (2000).

NOTE: The Court specifically differentiated such roadblocks from sobriety checkpoints, also indicated that its holding "does not affect the validity of . . . searches at places like airports and government buildings, where the need for such measures to ensure public safety can be particularly acute[;] . . ." and noted that it would in all likelihood sustain "an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route. . . ."

In judging reasonableness of a brief, information-seeking stop (checkpoint), the Court looks to the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty. *Illinois v. Lidster*, 540 U.S. 419 (2004).

NOTE: In *Lidster*, the reasonableness of a brief, information-seeking stop [checkpoint] was upheld where vehicle occupants, as members of the public, were asked for their assistance in providing information about a fatal hit-and-run crash which had occurred a week earlier at the same location and time of night and which in all likelihood had been committed by others.

Vehicle Searches—Incident to Arrest

Incident to and contemporaneous with a valid arrest, officers may search the entire passenger compartment of a vehicle, including any closed container(s) therein to discover instruments of a crime, contraband, evidence of a crime, or dangerous weapons. *New York v. Belton*, 453 U.S. 454 (1981).

Search incident to an arrest exception does not apply to an offense for which a person would normally be only issued a traffic citation, even if the officer may have probable cause to make the arrest. *Knowles v. Iowa*, 525 U.S. 113 (1998).

In many cases, as when a recent occupant is arrested for a traffic violation, there will be no reasonable basis to believe the vehicle contains relevant evidence. *Atwater v. City of Lago Vista*, 532 U.S. 318 (2001).

Search Incident to Arrest only authorizes police to search a vehicle incident to a recent occupant's arrest only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search. *Arizona v. Gant*, 556 U.S. 332 (2009).

Officers must generally secure a warrant before conducting a search of data on cell phones. The United States Supreme Court's holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. The United States Supreme Court's answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant. *Riley v. California*, 573 U.S. __, 134 S. Ct. 2473 (2014).

Vehicle Searches—Exigency

A police officer can search a motor vehicle and any container therein capable of carrying the object of the search without a warrant, if the officer has probable cause to believe that it is carrying contraband. This is based on the inherent mobility of a vehicle that can allow it to quickly travel outside the jurisdiction of the officers. *Carroll v. United States*, 267 U.S. 132 (1925).

The *Carroll* automobile exception does not require a separate finding of exigency in addition to a finding of probable cause; in cases where there was probable cause to search a vehicle, a search is not unreasonable if based on facts that would justify issuing a warrant, even though a warrant has not been actually obtained. *Maryland v. Dyson*, 527 U. S. 465 (1999).

NOTE: This may hold true even if the owner of the vehicle is in police custody at the time of the search; it is noteworthy, however, that the search in this case involved only an examination of the exterior of arrestee's vehicle. *Cardwell, Warden v. Lewis*, 417 U.S. 583 (1974).

NOTE: It does not matter if a container belongs to the driver or a passenger, as long as it is capable of containing the object of the search. *Wyoming v. Houghton*, 526 U.S. 295 (1999).

NOTE: Some states interpret their state constitutions to require probable cause and also exigent circumstances or another exception to the warrant requirement. *State v. Sterndale*, 139 N.H. 445 (1995).

Vehicle Searches—Inventory

When officers tow or otherwise take a vehicle into custody, if the police department has a policy requiring it, they may make a complete inventory of the contents of the vehicle in order to protect the owner's property and protect the police from accusations of theft. *South Dakota v. Opperman*, 428 U.S. 364 (1976).

The search may include any open or closed containers in the vehicle, if the department's policy specifically calls for this action. *United States v. Ross*, 456 U.S. 798 (1982).

Vehicle Searches—Consent Searches

Consent for a search is valid only if it is freely, voluntarily, and knowingly given. Officers are not required to inform the person that he has the right to refuse consent. *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973).

When deciding whether consent was voluntary or not, courts will consider three factors—the proximity in time between any illegal police conduct and the consent to search, the presence of any intervening circumstances, and the purpose and flagrancy of any official misconduct. *Brown v. Illinois*, 422 U.S. 590 (1975).

Police officers are permitted to ask a person in custody or control of a motor vehicle for consent to search the vehicle and the individual's person; if the person is illegally detained, however, when he consents to the search, the consent is tainted by the illegality and is ineffective to justify the search. *Florida v. Royer*, 460 U.S. 491 (1983).

NOTE: Articulable, reasonable suspicion of wrongdoing is not required in most jurisdictions in order to ask a person for consent to search, but New Jersey follows a more stringent rule under its state constitution, *State v. Carty*, 322 NJ Super 200, 753 A2d. 149 (2000).

NOTE: A growing body of state case law favors written waivers that contain a notice of the right of refusal. Some states have ruled that if a police officer is still holding the person's license and registration when asking for consent to search, the consent will be invalid unless the person was told of his right to refuse, *State v. Hight*, 146 N.H. 746, 781 A2d. 11 (2001).

Computer Checks of Registration Plate Numbers

The supreme courts in some states have held that random computer checks of passing vehicle's license plate numbers are not searches under the 4th Amendment or the state constitution. If check reveals the registered owner has a suspended license that provides reasonable suspicion for a traffic stop. *State v. Richter*, 145 N.H. 640, 765 A.2d. 687 (2000).

Community Caretaking

Whether a search and seizure is unreasonable within the meaning of the 4th Amendment depends upon the facts and circumstances of each case. It is permissible to search a vehicle pursuant to the police community caretaking functions, those that are totally divorced from the detection, investigation, or acquisition of evidence relating to the violation of a criminal statute. *Cady v. Dombrowski*, 413 U.S. 433 (1973).

NOTE: In *Dombrowski*, police removed defendant's car to a tow yard following a crash and defendant's DUI arrest. Defendant was a police officer in another jurisdiction; arresting police searched defendant's vehicle for his department-issued weapon to protect public safety to prevent the weapon from falling into untrained or malicious hands (*e.g.*, community care taking). Search found to be reasonable.

Some states recognize a "community caretaking exception" to the requirement of articulable, reasonable suspicion to justify a motor vehicle stop. Seizure of property by the police is justified by the community caretaking exception when it constitutes no more than a routine and good faith attempt, in the exercise of reasonable caution, to safeguard the defendant's own property. *State v. Psomiades*, 139 N.H. 480 (1995).

NOTE: Police officer's actions in removing valuables without a warrant from a car left by the side of the road at 3 a.m. constituted a legitimate caretaking function, and therefore did not violate the New Hampshire Constitution.

Driver's License

A driver's license is an "important interest" and cannot be taken away or denied without affording the person due process of law. *Bell v. Burson*, 402 U.S. 535 (1971).

Licensing authority may summarily suspend or revoke a license based on official records and prior to a preliminary hearing. *Dixon v. Love*, 431 U.S. 105 (1977).

Under implied consent, summary suspension of license based on refusal to submit to breath test upon DUI arrest is permissible; compelling interest in highway safety justifies summary suspension effective pending the outcome of the prompt post-suspension hearing available. *Mackey v. Montrym*, 443 U.S. 1 (1979).

An officer's affidavit for refusal under implied consent does not have to recite the reasonable grounds the officer had that the driver was DWI. *Illinois v. Batchelder*, 463 U.S. 1112 (1983).

NOTE: Some jurisdictions have ruled that Administrative License Suspension hearings are non-criminal in nature, that the Exclusionary Rule does not apply to them, and that the issue of probable cause to stop the vehicle therefore is not to be considered in such hearings. *Lopez v. Director of Motor Vehicles*, 145 N.H. 222, 761 A2d. 448 (2000).

Standardized Field Sobriety Tests (SFST)

It is not required to give the *Miranda* warnings to a motorist before asking him if he will submit to a chemical test or to a physical balance and coordination test, because you are not asking him to make incriminating statements. *South Dakota v. Neville*, 459 U.S. 553 (1983).

Need not provide Miranda prior to SFSTs. *Berkemer v. McCarty*, 468 U.S. 420 (1984).

Miranda affords protection against self-incrimination to persons under custodial interrogation. The Supreme Court distinguishes between testimonial and real or physical evidence when invoking the privilege. SFST constitute real or physical evidence; whereas requiring defendant to respond to specific questions is testimonial. A defendant's statements during administration / performance of SFST may not be testimonial and may, therefore, be admissible. In order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a witness against himself. *Pennsylvania v. Muniz*, 496 U.S. 582 (1990).

NOTE: In *Muniz*, responses made by defendant while officers conducted field sobriety tests were admissible, but after defendant received direct questions that could have been construed as custodial interrogation, *Miranda* warnings should have been given.

Implied Consent and Refusal

Where a driver refused a chemical test, this refusal could be admitted into evidence at the trial, and it did not violate his constitutional rights. *South Dakota v. Neville*, 459 U.S. 553 (1983); *Missouri v. McNeely, 569 U.S. __, 133 S. Ct. 1552 (2013).*

Some jurisdictions have found no due process violation even when a police officer fails to provide to a suspect notice of the consequences of his refusal. *Kanikaynar v. Sisneros*, 190 F.3d 1115 (10th Cir. 1999).

All 50 States have adopted implied consent laws that require motorists, as a condition of operating a motor vehicle within the State, to consent to BAC testing if they are arrested or otherwise detained on suspicion of a drunk-driving offense. *Missouri v. McNeely,* 569 U.S. __, 133 S. Ct. 1552 (2013) and *Birchfield v. North Dakota,* 579 U.S. __, 136 S. Ct. 2160 (2016).

NOTE: But some states' implied consent laws provide for NO testing if driver refuses (even if SW obtained), see *State v. Adee*, 241 Kan. 825, 740 P. 2d 611 (1987) citing *State v. Brunner*, 211 Kan. 596, 507 P. 2d 233 (1973)).

NOTE: Some states have determined that in order for consent to be valid, a driver must have the ability to ultimately refuse when requested to submit to a chemical test. In other words, without the ability to refuse, some states have deemed such consent to be coerced and disallowed the use at trial of subsequent test results. See *State v. Won*, 136 Haw. 292, 361 P.3d 1195 (2015) and *State v. Ryce*, 303 Kan. 899 (2016).

A refusal to submit to a blood test cannot be criminalized; a refusal to submit to breath can be a separate crime. *Birchfield v. North Dakota,* 579 U.S. __, 136 S. Ct. 2160 (2016).

NOTE: Some jurisdictions may equate breath test limited intrusion to urine or oral fluid tests.

NOTE: Some jurisdictions may charge a refusal offense (or equivalent) if a defendant refuses to submit to a blood test after a search warrant has been obtained.

Chemical Testing—Warrantless Searches

The natural dissipation of alcohol in the blood does not create a categorical per se exigency that justifies a warrantless search. *Missouri v. McNeely*, 569 U.S. __, 133 S. Ct. 1552 (2013).

A breath test, but not a blood test, may be administered as a search incident to a lawful DUI arrest. *Birchfield v. North Dakota*, 579 U.S. __, 136 S. Ct. 2160 (2016).

Chemical Testing—Right to Attorney Prior to Test

Courts are split as to whether the taking of a sample of a defendant's blood, breath or urine, even under implied consent, is a "critical stage of a criminal proceeding" at which a 6th Amendment right to counsel is applicable. See *Sites v. State*, 300 Md. 702, 481 A. 2d 192 (1984) and *Heles v. South Dakota*, 530 F. Supp. 646 (SD), vacated as moot, 682 F. 2d 201 (CA8 1982). Some courts have found a right to counsel based on state law, e.g., State v. Fitzsimmons, 94 Wash. 2d 858, 620 P. 2d 999 (1980), or on general due process guarantees, see, e.g., State v. Newton, 291 Ore. 788, 636 P. 2d 393 (1981) (en banc plurality).

Chemical Testing—Saving Breath Sample for Defendant

The due process clause of the 14th Amendment does not require that law enforcement agencies preserve breath samples in order to introduce the results of breath-analysis tests at trial. *California v. Trombetta*, 467 U.S. 479 (1984).

NOTE: State courts and legislatures, of course, remain free to adopt more rigorous safeguards governing the admissibility of scientific evidence than those imposed by the Federal Constitution. See e. g., Lauderdale v. State, 548 P. 2d 376 (Alaska 1976); City of Lodi v. Hine, 107 Wis. 2d 118, 318 N. W. 2d 383 (1982).

The U.S. Constitution does not require the prosecution to preserve a breath sample so that a defendant can have it analyzed at a later time. *California v. Trombetta*, 467 U.S. 479 (1984). NOTE: In some states, such as New Hampshire, the State Supreme Court has ruled that under the State Constitution, a second sample is required. *State v. Cornelius*, 122 N.H. 925, 452 A.2d. 464 (1982).

APPENDIX A: BIBLIOGRAPHY OF RESOURCES






Cover Images Credits:
Photo Credit #1: Takepart website. This May Be a New Model for Community Policing

http://www.takepart.com/sites/default/files/styles/large/public/Camden.jpg

(Photo: Andrew Burton/Getty Images). Website: December 23, 2016.

Photo Credit #2: Police Officer Holds Baby: https://stock.adobe.com/nl/search?filters%5Bcontent_type%3Aphoto%5D=1&filters%5Bcontent_type%3Aillustration%5D=1&filters%5Bcontent_type%3Azip_vector%5D=1&filters%5Bcontent_type%3Avideo%5D=1&filters%5Bcontent_type%3Atemplate%5D=1&filters%5Bcontent_type%3A3d%5D=1&safe_search=1&ca=0&similia_id=14491965

Website: December 23, 2016.

Photo Credits: #3 https://unsplash.com/@_th4d_ Thaddaeus Lim; From Unsplash Website. December 23, 2016.

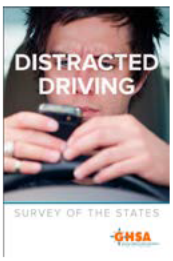
Photo Credit: #4 Delaware State Police. Seifert, Personal collection. December 23, 2016.

This Bibliography of Resources serves as supplementary information providing current resources available to assist law enforcement officers with further research and additional information. This part of the Resource Guide includes contemporary information available to assist leaders in their efforts to address five main themes of traffic safety. These five themes are divided into four sections:

1. **Section One: Reduction of Traffic Crashes**
2. **Section Two: Officer Safety**
3. **Section Three: Commercial Vehicles and Transportation of Hazardous Materials**
4. **Section Four: Emerging and Critical Issues**

The bibliography encompasses books, academic journals, downloadable archived research materials, websites, webinars, podcasts, magazine articles and more. After reviewing these resources, you are encouraged to look at the bibliography for each item as this will provide additional helpful research materials. The resources serve to point the reader to promising practices, strategies, research, and lessons learned for enhancing traffic safety.

SECTION ONE: REDUCING TRAFFIC CRASHES



2013 Distracted Driving: Survey of the States **(Governors Highway Safety Association, 2013)**

Website Link: http://www.ghsa.org/resources/2013distracted

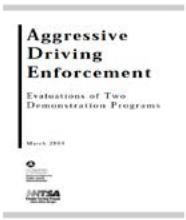
Abstract: The Governors Highway Safety Association (GHSA) provides this website and a downloadable publication which outlines efforts to combat distracted driving. Highlights of the report include the latest information on laws and law enforcement, public education efforts, partnerships with other organizations and data.



A New Tool to Assess the Costs and Effectiveness of Traffic Crash Interventions **(Liisa Ecola and Jeanne S. Ringel, 2016)**

Website Link: http://www.rand.org/blog/2016/04/a-new-tool-to-assess-the-costs-and-effectiveness-of.html#reductions3

Abstract: This April 2016 blog post from the Rand Corporation provides details about an online tool called Motor Vehicle Prioritizing Interventions and Cost Calculator for States (MV PICCS) that generates state-specific cost-effectiveness estimates for traffic crash interventions. MV PICCS allows users to compare 14 interventions on cost and effectiveness. The tool is available for free at www.cdc.gov/motorvehiclesafety/calculator.



Aggressive Driving Enforcement: Evaluation of Two Demonstration Programs (Jack Stuster, 2004)

Website Link: https://www.nhtsa.gov/document/aggressive-driving-enforcement

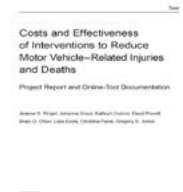
Abstract: This report presents the results of a study conducted for the National Highway Traffic Safety Administration (NHTSA) to assess the effects of two programs that were implemented to reduce the incidence of aggressive driving. The programs were conducted by the Marion County Traffic Safety Partnership (a consortium of agencies in the vicinity of Indianapolis, Indiana), and The Tucson, Arizona, Police Department. Study results suggest that limited resources might be better spent on officer labor than on publicity, and that focusing enforcement responsibility on a small team assigned full-time to the special enforcement patrols might be more effective than sharing the responsibility among a large number of officers as occasional overtime duty.



Compendium of Traffic Safety Research Projects 1985-2013 **(National Highway Traffic Safety Administration, 2014)**

Website Link: http://www.nhtsa.gov/staticfiles/nti/pdf/CompendiumTrafficSafetyResearchProjects1985-2013.pdf

Abstract: The Compendium is a NHTSA summary of research on alcohol-involved driving, drug-involved driving, occupant protection (e.g., seatbelts, and child safety seats), speed and other unsafe driving behaviors, motorcyclist safety, pedestrian and bicyclist safety, older driver safety, novice and young driver safety, fatigue and distraction, and emergency medical services.



Costs and Effectiveness of Interventions to Reduce Motor Vehicle–Related Injuries and Deaths: Project Report and Online-Tool Documentation **(Jeanne S. Ringel, Johanna Zmud, Liisa Ecola, Christina Pavis and Gregory S. Jones, 2015)**

Website Link: http://www.rand.org/pubs/tools/TL144z1.html

Abstract: This report from the Rand Corporation documents the approach, data, and assumptions used to produce an online tool that allows state decision makers to assess the costs and effectiveness of implementing up to 14 interventions and to select those most effective in reducing deaths and injuries from motor vehicle crashes for a given implementation budget. It also provides examples of how costs and benefits were identified for certain interventions, as well as instructions about using the tool in various modes of analysis. The tool was developed for and is hosted by the Centers for Disease Control and Prevention's National Center for Injury Prevention and Control.



Countermeasure Strategies for Pedestrian Safety. **(Federal Highway Administration and the Pedestrian and Bicycle Information Center, 2015)**

Website Link: http://www.pedbikeinfo.org/training/webinars_PSAP_countermeasurestrategies.cfm

Abstract: The Federal Highway Administration and the Pedestrian and Bicycle Information Center developed this webinar series. The webinars provide participants with an in-depth exploration of some of the countermeasures and

design strategies that can be implemented to improve pedestrian safety. Each of the 12 sessions feature detailed information about countermeasures and design strategies, supporting research and guidance, as well as case studies highlighting examples of implementation from around the United States.



Countermeasures that Work: A Highway Safety Countermeasure Guide for State Highway Safety Offices Eighth Edition, 2015. **(Arthur Godwin, Libby Thomas, Bevan Kirley, William Hall, Natalie O'Brien and Kate Hill, 2015)**

Website Link: www.nhtsa.gov/staticfiles/nti/pdf/812202-CountermeasuresThatWork8th.pdf

Abstract: This guide is a basic reference to assist State Highway Safety Officers in selecting effective, science-based traffic safety countermeasures for major highway safety problem areas.



Eyes on the Road: Searching for Answers to the Problem of Distracted Driving **(Sarah Karush, Insurance Institute for Highway Safety, 2014)**

Website Link: https://www.iihs.org/news/detail/searching-for-answers-to-the-problem-of-distracted-driving

Abstract: This resource from the Insurance Institute for Highway Safety details research by the Institute and the Virginia Tech Transportation Institute (VTTI). The Institute found drivers' near-crash and crash risk changes as their cellphone usage patterns change and how cellphone use fits in with other driver behavior and affects attention to the road. The research confirms that frequent cellphone users have more near misses or crashes.



Florida's Pedestrian & Bicycle Focused Initiative **(State of Florida, 2016)**

Website Link: http://www.alerttodayflorida.com/

Abstract: In 2011, Florida's Department of Transportation developed a very successful Bicycle/Pedestrian Focused Initiative working towards the goal of increasing awareness and decreasing fatalities of bicyclists and pedestrians. This website has information on significant accomplishments, the outreach and media campaign, education, engineering and enforcement as well as a compendium of resources and research related to pedestrian and bicycle safety information.



Graduated Driver Licensing Research Review **(AAA Foundation for Traffic Safety, 2012)**

Website Link: https://aaafoundation.org/graduated-driver-licensing-research-review-2010-present/

Abstract: This research from the AAA foundation is the latest in a series of reviews of research on graduated driver licensing (GDL) published in the Journal of Safety Research. The intent is to keep researchers and policy makers current regarding the existing state of knowledge about GDL, and to identify information gaps and areas where clarification of research findings is needed.



High-Visibility Education and Enforcement (HVEE) Pilot Project **(Brad Wentlandt, 2016)**

Website Link: http://www.policechiefmagazine.org/high-visibility-education-and-enforcement-hvee-pilot-project/#sthash.dY6w0hlv.dpuf

Abstract: This resource details the high-visibility education and enforcement project. Four U.S. states participated in the IACP-led effort with programs addressing specific local safety concerns. The HVEE approach offers an evidence-based, data-driven problem-solving approach by using proactive public education campaigns to raise awareness of the identified safety issue, followed by targeted enforcement involving multiple law enforcement agencies.



Impact of the Legalization and Decriminalization of Marijuana on the DWI System: Highlights from the Expert Panel Meeting **(NHTSA and Governor's Highway Safety Association, 2017)**

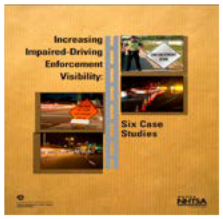
Website Link: http://bit.ly/ncrep062617#sthash.EFqskPIh.dpuf

Abstract: The legalization of marijuana for medicinal or recreational use at the state level has the potential to have downstream effects on the entire impaired driving system. In its first completed research project, the National Cooperative Research and Evaluation Program (NCREP) convened a group of national experts, representing states that had enacted such laws, to discuss these consequences and identify issues for consideration by other states that may be considering the adoption of these laws. *Impact of the Legalization and Decriminalization of Marijuana on the DWI System* is the culmination of these deliberations. It outlines key factors for consideration in seven topic areas: law enforcement, prosecution, adjudication, forensics, data, State Highway Safety Offices (SHSOs) and public outreach.



***Implementing DDACTS in Baltimore County: Using Geographic Incident Patterns to Deploy Enforcement* (Howard Hall and Emily N. Puls, 2010)**

Abstract: In 2008, the Baltimore County Police Department began implementation of Phase I of its DDACTS (Data-Driven Approaches to Crime and Traffic Safety) initiative. This article examines in detail how and why the Baltimore County Police Department chose to incorporate and implement the DDACTS model as part of its overall data-driven policing strategy. Results from the evaluation of Baltimore County's use of DDACTS are encouraging and show that DDACTS can be used to efficiently and effectively deploy scarce police resources.



***Increasing Impaired-Driving Enforcement Visibility: Six Case Studies* (James Fell. A. Scott McKnight and Amy Auld-Owens, 2013)**

Website Link: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/811716.pdf

Abstract: This report presents six case studies of "high-visibility enforcement" (HVE) which are law enforcement efforts aimed at deterring unsafe driving behavior by increasing the public's perception of being caught, arrested, and prosecuted. The report is intended to provide information on impaired driving HVE programs for regional, State and local agencies considering incorporating HVE strategies into their efforts to curb impaired driving or to modify existing HVE programs.



***Law Enforcement Executive's Guide to High Visibility Enforcement* (Maryland Chiefs of Police Association, 2016)**

Website Link: http://www.nlelp.org/wp-content/uploads/2016/09/LE_Exec_Guide.pdf

Abstract: The Maryland Chiefs of Police Association, Maryland Sheriff's Association, and the Maryland Highway Safety Office recently collaborated on the publication of the "Law Enforcement Executive's Guide to High Visibility Enforcement," which can be found here: http://www.nlelp.org/wp-content/uploads/2016/09/LE_Exec_Guide.pdf



***Marijuana, Other Drugs, and Alcohol Use by Drivers in Washington* State (Anthony Ramirez, Amy Berning, Katherine Carr, Michael Scherer, John H. Lacey, Tara Kelley-Baker, and Deborah A. Fisher, 2016)**

Website Link: https://www.nhtsa.gov/staticfiles/nti/pdf/812299-WashingtonStatedrugstudy.pdf

Abstract: In Washington State legal sales of marijuana began July 8, 2014. A voluntary, anonymous roadside study was conducted to assess the prevalence of drivers testing positive for alcohol and other drugs, including marijuana, on Washington's roads. Data was collected in three waves, before implementation of legal sales, about 6 months after implementation, and 1 year after implementation. This research provides important information on the impact of data on marijuana use by drivers.



***Older Drivers Safety Program* (Georgia Department of Public Health, 2017)**

Website Link: https://dph.georgia.gov/ODS

Abstract: Funded by the Georgia Governor's Office of Highway Safety, this website provides information for law enforcement regarding several initiatives to reduce the number of injuries and fatalities experienced by older drivers.



***Pedestrians and bicyclists* (The Insurance Institute for Highway Safety Highway Loss Data Institute, 2017)**

Website Link: http://www.iihs.org/iihs/topics/t/pedestrians-and-bicyclists/qanda

Abstract: This resource from the Insurance Institute for Highway Safety provides important information on fatality facts, public presentations, research and policy related information regarding pedestrians and bicyclists.



***Police Training to Spot Marijuana Use* (Oriana Durand, 2017)**

Website Link: http://www.telegram.com/news/20170101/police-training-to-spot-marijuana-use

Abstract: This January 2017 article which was published in the Telegram & Gazette (Worcester, Massachusetts) described the challenges faced by law enforcement with the detection of impaired drivers. The Drug Recognition Expert (DRE) program was described and police officers detailed how it can be used to help determine if a motorist was under the influence of drugs.



***Progress in Teenage Crash Risk During the Last Decade.* (Susan A. Ferguson; Eric R. Teoh; Anne T. McCartt, 2007)**

Journal of Safety Research, v38 n2

Website Link: http://www.sciencedirect.com/science/journal/00224375/38/2

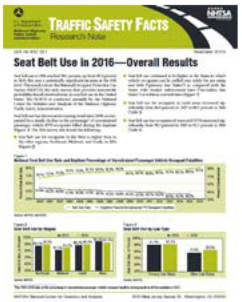
Abstract: This research examined the most recent data on teenagers' fatal and nonfatal crashes in the United States to determine current crash rates as well as changes in crash rates during the past decade for calendar years 1996 and 2005 were extracted for fatal crashes from the Fatality Analysis Reporting System and for police-reported crashes.



***Recommendations for Toxicological Investigation of Drug-Impaired Driving and Motor Vehicle Fatalities* (Barry K. Logan, et al, 2013)**

Website Link: https://academic.oup.com/jat/article-lookup/doi/10.1093/jat/bkt059

Abstract: This research is presented in the Journal of Analytical Toxicology. The report describes the review and update of a set of minimum recommendations for the toxicological investigation of suspected alcohol and drug-impaired driving cases and motor vehicle fatalities involving drugs or alcohol. The recommendations have the goal of ensuring that a consistent set of data regarding the most frequently encountered drugs linked to driving impairment is collected for practical application in the investigation of these cases and to allow epidemiological monitoring and the development of evidence-based public policy on this important public safety issue.



***Seatbelt Use in 2016 – Overall Results* ((National Highway Traffic Safety Administration, 2016)**

Website Link: https://crashstats.nhtsa.dot.gov/#/

Abstract: This NHTSA Traffic Safety Facts bulletin reports on seatbelt use in the United States where use has reached its highest level since the federal government began regular surveys in 1994.



***Smart Policing and Data-Driven Approaches to Crime and Traffic Safety (DDACTS) Webinar.* (Chief Howard Hall and Chip Coldren, et al, 2014)**

Website Link: http://www.strategiesforpolicinginnovation.com/tta/webinars/spi-data-driven-approaches-crime-and-traffic-safety

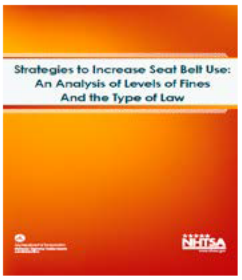
Abstract: The Smart Policing Initiative hosted a webinar on Data-Driven Approaches to Traffic and Crime Safety (DDACTS). This was an online, interactive seminar aimed at engaging the SPI community in a focused discussion around recent evidence regarding the effectiveness of DDACTS, how DDACTS reflects Smart Policing Principles, and DDACTS information resources available to police agencies. Four police agencies also discussed their experiences with DDACTS, including Roanoke County (VA), Metro Nashville (TN), Mesa (AZ), and Shawnee (KS).



***State of Knowledge of Alcohol-Impaired Driving: Research on Repeat DWI Offenders* (John H. Lacey and Ralph K. Jones, 2000)**

Website Link: https://one.nhtsa.gov/people/injury/research/pub/Alcohol-ImpairedDriving.html

Abstract: This study reviews the scientific literature since 1990 relating to drivers who have been convicted more than once of driving while impaired by alcohol (DWI). It covers the role of such drivers in alcohol-related crashes, their characteristics, and the nature and effectiveness of countermeasures designed to reduce their alcohol-crash involvement. The review was performed as part of a larger review of the state of knowledge of alcohol-impaired driving at the millennium.



***Strategies to Increase Seatbelt Use: An Analysis of Levels of Fines and the Type of Law* (James L. Nichols, A. Scott Tippetts, James C. Fell, Amy Auld-Owens, Connie H. Wiliszowski, Philip W. Haseltine, and Angela Eichelberger, *2010*)**

Website Link: www.nhtsa.gov/staticfiles/nti/occupant_protection/pdf/811413.pdf

Abstract: The main objectives of this study were to determine the relationships between seatbelt use in the States and (1) the type of seatbelt law enforcement (primary versus secondary), and (2) seatbelt fine levels. The study examined law type and levels of fines as predictors of seatbelt use for two time periods (1997 to 2002 and 2003 to 2008) using panel regression analyses. Two outcome measures were examined: seatbelt use among front-seat occupants over age 8 killed in passenger vehicle crashes from the Fatality Analysis Reporting System (FARS) and the observed statewide seatbelt use of front-seat occupants in passenger vehicles.



***Teenagers: Driving Carries Extra Risk for Them* (The Insurance Institute for Highway Safety Highway Loss Data Institute, 2016)**

Website Link: http://www.iihs.org/iihs/topics/t/teenagers/hldi-research

Abstract: The Insurance Institute for Highway Safety Highway Loss Data Institute maintains this website with links to state laws; fatality facts; public presentations; regulatory and legislative policy; HLDI research and Q & A's.



***The Roadway Safety Guide: A Primer for Community Leaders* (Roadway Safety Foundation, 2014)**

Website Link: https://www.roadwaysafety.org/programs/roadway-safety-guide

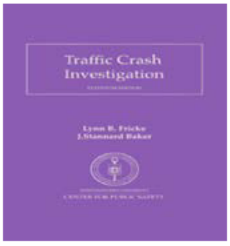
Abstract: The Roadway Safety Foundation is a non-profit educational organization charted in 1995 by the American Highway Users Alliance working with private and public sector safety partners to reduce fatalities attributed to roadway conditions. The Roadway Safety Guide is designed to provide community leaders and elected officials with basic information to improve roadway safety in their communities.



***Traffic Safety Initiatives: Motorcycle Safety* (Samuel Capogrossi, 2017)**

Website Link: https://www.policechiefmagazine.org/traffic-safety-initiatives-motorcycle-safety/

Abstract: This 2017 article from the Police Chief magazine highlights key statistics related to motorcyclists on U.S. roadways. It summarizes ongoing research findings of NHTSA, GHSA, FHWA and best practices to improve motorcycle safety. The article reports that some of the key findings are the need to ensure motorcycle riders are properly trained and licensed; the need to remove alcohol-impaired operators from the roads; the need to increase other motorists' awareness of motorcyclists by increasing visibility and the need to educate motorcyclists on the importance of wearing approved helmets and clothing.



***Traffic Crash Investigation* (J. Stannard Baker and Lynn B. Fricke, 2014)**

Website Link: https://sps.northwestern.edu/center-for-public-safety/shop/product.asp?intProdID=431

Abstract: *Traffic Crash Investigation, 11th Edition* is a comprehensive collection of the most important techniques and definitions essential for developing an accurate picture of motor vehicle crashes. Crash investigators who practice these techniques provide information that ultimately saves lives and reduces monetary losses. Considered the definitive standard by attorneys, prosecutors and judges, law enforcement officers, engineers and other safety groups, the 11th edition is a major update of the text.



***Traffic Safety Innovations: How Agencies Use the National Law Enforcement Challenge to Zero In on Traffic Safety Issues* (Bethany Peterson and Matt Alderton, 2016)**

Website Link: http://www.policechiefmagazine.org/traffic-safety-innovations-how-agencies-use-the-national-law-enforcement-challenge-to-zero-in-on-traffic-safety-issues/

Abstract: This resource provides a summary of the National Law Enforcement Challenge a traffic safety recognition program aimed at the issues of impaired driving, occupant protection, and speeding. The article describes law

enforcement programs which serve as a collection of success stories and recommendations from agencies that have implemented best practices to address a traffic safety problem specific to their community or in support of the state's highway safety strategic plan. Traffic safety initiatives in nine police departments were described.



***Traveling the Three Lanes on the Road to Zero* (National Highway Traffic Safety Administration, 2016)**

Website Link: https://www.nhtsa.gov/press-releases/traveling-three-lanes-road-zero

Abstract: This resource briefly introduces the new strategic plan of NHTSA. NHTSA has adopted "three lanes to zero to help deliver a future free of motor vehicle fatalities: Proactive Vehicle Safety; Advanced Vehicle Safety Technologies and addressing Human Factors like drunk, drugged, distracted and drowsy driving.



***Using Cost-Effectiveness Analysis to Prioritize Spending on Traffic Safety* (Liisa Ecola, Benjamin Saul Batorsky and Jeanne S. Ringel, 2015)**

Website Link: http://www.rand.org/pubs/tools/TL144z1.html

Abstract: This report examines how traffic safety funding could be spent to reduce motor vehicle crash–related injuries and deaths. Specifically, it assesses three issues: the most cost-effective interventions at the national and state levels, whether to allocate incremental funding increases to all states or spend the funds in targeted states, and how best to allocate funds that target drunk driving.

SECTION TWO: OFFICER SAFETY



IACP Officer Safety and Wellness Website

Website Link: http://www.theiacp.org/COSW

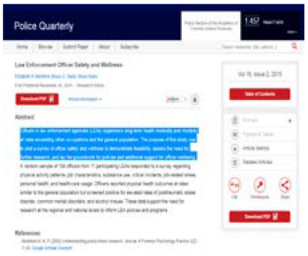
Abstract: Comprehensive website hosted by the IACP which offers tools, model policies, reports and publications, and articles and blog posts related to officer safety and wellness.



Is Today Your Day? (IACP and the New York State Police, 2010)

Website Link: https://youtu.be/Lv_viNAylqc

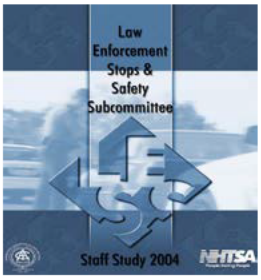
Abstract: This YouTube video was produced by the Ohio State Highway Patrol and the IACP. It is a twenty-two minute video promoting officer safety to reduce police officer deaths and injuries. It is suitable for roll call training.



Law Enforcement Officer Safety and Wellness (Elizabeth A. Mumford, Bruce G. Taylor and Bruce Kubu, 2014)

Website Link: https://journals.sagepub.com/doi/abs/10.1177/1098611114559037?journalCode=pqxa

Abstract: Officers in law enforcement agencies (LEAs) experience long-term health morbidity and mortality at rates exceeding other occupations and the general population. The purpose of this study was to pilot a survey of officer safety and wellness to demonstrate feasibility, assess the need for further research, and lay the groundwork for policies and additional support for officer wellbeing.



Law Enforcement Stops and Safety Subcommittee Staff Study (IACP and NHTSA, 2004)

Website Link: http://dnn9ciwm8.azurewebsites.net/TrafficOfficerSafetySubcommittee

Abstract: This 2004 Staff Study Report documents the work to date of the IACP Law Enforcement Stops and Safety Subcommittee. It includes technology, practices, and research related to improving officer safety and preventing police vehicle crashes. Recommendations are included at the end of each section of the report as benchmarks against which to measure future successes to improve the safety of police vehicles, highway environment and design, and traffic stop practices.



Officer Safety: Reducing Injuries and Fatalities for the Law Enforcement Officer on the Front Lines of Traffic Safety (Sheriff John Whetsel and Ed Hutchison, 2015)

Podcast from the National Law Enforcement Liaison Program

Website Link: http://www.nlelp.org/podcast-sheriff-john-whetsel-and-ed-hutchison-on-officer-safety/

Abstract: During the GHSA 2015 Annual Meeting, the National Law Enforcement Liaison Program (NLELP) sat down with Sheriff John Whetsel, Sheriff of Oklahoma County, Oklahoma and chair of the National Sheriffs Association Traffic Safety Committee, and Ed Hutchinson, Director of Traffic Safety for the National Sheriffs Association, to talk about ways to reduce injuries and fatalities for the law enforcement officers who are on the front lines of traffic safety. This podcast, as well as the NLELP website, offers information on officer safety concerns, best practices, case law, occupant protection, and multi-state and regional initiatives related to traffic safety.



The Influence of Officer Positioning on Movement During a Threatening Traffic Stop Scenario (William J. Lewinski, PhD, Jennifer L. Dysterheft, Dawn A. Seefeldt, MA, Robert W. Pettitt, PhD, 2013)

Website Link: https://www.forcescience.org/2013/03/the-influence-of-officer-positioning-on-movement-during-a-threatening-traffic-stop-scenario/

Abstract: This research study uses science to evaluate officer responses to deadly threats encountered during traffic stops. Topics covered in the study include passenger-side approaches; mitigation of hazards on traffic stops; officer position relative to the B-Pillar of a vehicle on tactical responses to a lethal threat and origination of threats from within the stopped vehicle.



They Don't See You **(IACP and Ohio State Highway Patrol, 2014)**

Website Link: http://dnn9ciwm8.azurewebsites.net/TrafficOfficer-SafetySubcommittee

Abstract: This YouTube video was produced by the Ohio State Highway Patrol and the IACP. It is a ten minute video highlighting officer safety considerations and is suitable for roll call training.

Solutions for Safer Traffic Stops **(Richard J. Ashton, 2004)**

Website Link: http://www.policechiefmagazine.org/solutions-for-safer-traffic-stops/



Abstract: This Police Chief magazine article reports on the findings and recommendations to date of the International Association of Chiefs of Police's Law Enforcement Stops and Safety Subcommittee (LESSS), which has been assigned the task of improving officer safety during traffic stops and other roadside contacts.

SECTION THREE: COMMERCIAL VEHICLES AND TRANSPORTATION OF HAZARDOUS MATERIALS



***Best Practices and Lessons Learned in Commercial Vehicle Enforcement: A Perspective from the Ohio State Highway Patrol* (Colonel Paul A. Pride, 2015)**

Website Link: https://www.theiacp.org/news/blog-post/best-practices-and-lessons-learned-in-commercial-vehicle-enforcement-a-perspective-1

Abstract: This IACP Blog article details the efforts of the Ohio State Highway Patrol in addressing commercial vehicle enforcement safety. Colonel Paul Pride, Superintendent of the Highway Patrol, provides best practices around the Road Watch 100 campaign and lessons learned.



***Best Practices and Lessons Learned in Commercial Vehicle Enforcement: A Perspective from the Tennessee Highway Patrol* (IACP, 2015)**

Website Link: https://theiacpblog.org/2015/03/23/best-practices-and-lessons-learned-in-commercial-vehicle-enforcement-a-perspective-from-the-tennessee-highway-patrol/

Abstract: The IACP recognized the Tennessee Highway Patrol with the Commercial Vehicle Enforcement Award in 2005 and 2014. The Highway Patrol has been a leader in innovative commercial vehicle enforcement strategies. In this article, Colonel Tracy Trott, head of the Highway Patrol, provided best practices and lessons learned.



***Commercial Motor Vehicle Awareness Training Guide* (Federal Motor Carrier Safety Administration, 2011)**

Website Link: https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/docs/CMV-Awareness-Training-Guide.pdf

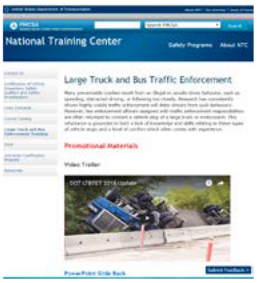
Abstract: The FMCSA provides this Training Guide to provide law enforcement officers with the safety and enforcement information for handling crashes and traffic enforcement involving commercial vehicles and buses. The Guide also provides information on the FMCSA training course available from officers from state, local and county law enforcement agencies.



***Fast Five Checklist for Large Truck and Bus Enforcement* (FMCSA and IACP, undated)**

Website Link: http://dnn9ciwm8.azurewebsites.net/large-trucks-and-buses

Abstract: The Federal Motor Carrier Safety Administration and the IACP collaborated on this checklist to assist police officers when conducting enforcement on large trucks and buses.



***Large Truck and Bus Traffic Enforcement Training* (FMCSA, 2016)**

Website Link: https://www.fmcsa.dot.gov/national-training-center/large-truck-and-bus-traffic-enforcement

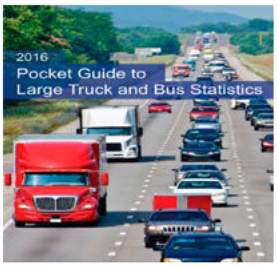
Abstract: This FMCSA website provides information on the Large Truck and Bus Traffic Enforcement Training program. Developed by the National Training Center in collaboration with law enforcement, the training is designed to enhance officers' knowledge about the dangers of unsafe driving by large trucks and buses. The training is available free to all law enforcement agencies and officer, and formatted to be delivered either on line, as a one hour, instructor-led training or divided into short segments for delivery during roll-call.



***Regular Traffic Enforcement Can Play a Crucial Role in Defining Commercial Vehicle Safety* (Jack Van Steenburg, 2014)**

Website Link: https://www.policechiefmagazine.org/regular-traffic-enforcement-can-play-a-crucial-role-in-defining-commercial-vehicle-safety/

Abstract: In this article, Jack Van Steenburg, Assistant Administrator and Chief Safety Officer, Federal Motor Carrier Safety Administration, provides information on the importance of daily traffic enforcement by police officers. The importance of changing commercial vehicle driver behavior is linked to the reduction of crashes and saving lives.



Pocket Guide to Large Truck and Bus Statistics **(Federal Motor Carrier Safety Administration, 2016)**

Website Link: **http://ntl.bts.gov/lib/59000/59100/59189/2016_Pocket_Guide_to_Large_Truck_and_Bus_Statistics.pdf**

Abstract: The FMCSA Pocket Guide is a compilation of statistics from the overall state of the industry to enforcement activity. It also provides details on traffic violations and other incidents, the costs of crashes, and more.



Saving Lives by Citing Truck and Bus Violations **(Stephen A. Keppler, 2011)**

Website Link: **https://www.policechiefmagazine.org/saving-lives-by-citing-truck-and-bus-violations/**

Abstract: In this article, Stephen A. Keppler, Executive Director, Commercial Vehicle Safety Alliance, describes the importance of the importance of traffic enforcement. The article also advocates raising the level of awareness on performance and driving behavior of those driving commercial vehicles and buses.

SECTION FOUR: EMERGING AND CRITICAL ISSUES



De-policing and Crime in the Wake of Ferguson: Racialized Changes in the Quantity and Quality of Policing Among Missouri Police Departments **(John A. Shjarback, David C. Pyrooz, Scotte E. Wolfe, and Scott H. Decker, 2017)**

Website Link: http://www.sciencedirect.com/science/article/pii/S0047235217301289

Abstract: This study explored whether police departments have engaged in "de-policing"—withdrawal from active police work—in response to unprecedented levels of negative attention, as well as the correlates of changes in police behavior.



Police Behavior During Traffic and Street Stops, 2011 **(Lynn Langton and Matthew Durose, 2011. Revised 2016)**

Website Link: https://www.bjs.gov/content/pub/pdf/pbtss11.pdf

Abstract: This Bureau of Justice Statistics report examines the characteristics and experiences of persons age 16 or older who were stopped by police during traffic and street stops, and their perceptions of police behavior and response during these encounters. It describes the outcomes of traffic and street stops by the reason for the stop; demographic characteristics of the persons stopped; race or Hispanic origin of the officers; and whether a ticket was issued, a search was conducted, or force was used. It also describes variations in perceptions of the police across characteristics and outcomes of traffic and street stops.



Preparing for a Future with Autonomous Vehicles **(Kevin Davis, 2016)**

Website Link: http://www.policechiefmagazine.org/preparing-for-a-future-with-autonomous-vehicles/?ref=8d4979dd5a2e9dff409434b4ad41d03e

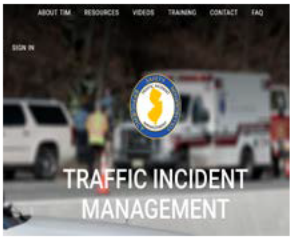
Abstract: This Police Chief magazine article reports on the many evolving issues that a world with autonomous vehicles will bring to society. Kevin Davis, a Captain with the California Highway Patrol, discusses the key issues and the potential impact upon traffic safety and police leaders.



Procedural Justice: Voice, Neutrality, Respect and Trustworthiness. **(California Commission on Peace Officer Standards and Training (POST), 2016)**

Website Link: https://post.ca.gov/did-you-know-procedural-justice.aspx

Abstract: This three minute California Commission on Peace Officer Standards and Training (POST) training video emphasizes the four tenets of Procedural Justice: Voice, Neutrality, Respect, and Trustworthiness. These tenets are modeled by the officer during a traffic stop and conversation with the driver of the stopped vehicle. This video would serve as an excellent roll call or in-service training video for police officers.



Traffic Incident Management – TIM Training and Capacity Building Videos and Related Resources **(New Jersey Department of Transportation, 2017)**

Website Link: http://www.njtim.org/NJTIM/

Abstract: This website is hosted by the New Jersey Department of Transportation. It provides excellent information on Traffic Incident Management. Law enforcement officers can review the helpful training videos as well as review various resources and sign up for TIM training held in New Jersey.



Understanding and Applying Traffic Incident Management **(Joseph A. Farrow and Daniel G. Sharp, 2015)**

Website Link: http://www.policechiefmagazine.org/understanding-and-applying-traffic-incident-management/

Abstract: This Police Chief magazine article provides an excellent overview of the primary concepts of traffic incident management.

APPENDIX B: ASSOCIATIONS AND COMMITTEES

The following is a listing of the associated groups currently active in the traffic safety field, together with a brief description of their administrative organization and relationship.

A.L.E.R.T. International

Website Link: http://www.alertinternational.com/?s=A.L.E.R.T.+International

A.L.E.R.T. International is dedicated to the encouragement and correlation of research and development as well as the sharing of information, ideas and innovations in the area of emergency vehicle response operation. Additionally, A.L.E.R.T.'s mission is to provide assistance to states in establishing effective and defensible standards for employment and training of law enforcement officers in the field of emergency vehicle operations. Another aspect of the mission is the promotion of a positive, professional image of emergency response trainers.

American Association of Motor Vehicle Administrators (AAMVA)

Website Link: http://www.aamva.org/

Founded in 1933, AAMVA represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws. AAMVA's programs encourage uniformity and reciprocity among the states and provinces. The association also serves as a liaison with other levels of government and the private sector. Its development and research activities provide guidelines for more effective public service. AAMVA's membership includes associations, organizations and businesses that share an interest in the association's goals.

AAMVA has the **Law Enforcement Standing Committee** within the association. This committee inspires collaboration between law enforcement and Driver/Motor Vehicle Administrators to improve highway and public safety. The Committee has the following goals:

1. Increase law enforcement participation in AAMVA conferences, working groups, and other initiatives.
2. Provide and promote uniformity and consistency through the development of standards, model programs and best practices.
3. Promote the exchange of challenges and successes in implementing technologies, sharing information, and with other contemporary law enforcement issues.

The American Association of State Highway and Transportation Officials (AASHTO)

Website Link: http://www.transportation.org/

The American Association of State Highway and Transportation Officials (AASHTO) is a standards setting body which publishes specifications, test protocols and guidelines which are used in highway design and construction throughout the United States. AASHTO has the **Standing Committee on Highway Traffic Safety** within the Association.

Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA)

Website Link: http://www.calea.org

The Commission on Accreditation for Law Enforcement Agencies, Inc., (CALEA®) was created in 1979 as a credentialing authority through the joint efforts of law enforcement's major executive associations the International Association of Chiefs of Police (IACP); National Organization of Black Law Enforcement Executives (NOBLE); National Sheriffs' Association (NSA); and the Police Executive Research Forum (PERF). The purpose of CALEA's Accreditation Programs is to improve the delivery of public safety services, primarily by: maintaining a body of standards, developed by public safety practitioners, covering a wide range of up-to-date public safety initiatives; establishing and administering an accreditation process; and recognizing professional excellence.

Council of State Governments (CSG)

Website Link: http://www.csg.org/

Founded in 1933, The Council of State Governments is our nation's only organization serving all three branches of state government. CSG is a region-based forum that fosters the exchange of insights and ideas to help state officials shape public policy. This offers unparalleled regional, national and international opportunities to network, develop leaders, collaborate and create problem-solving partnerships. **The mission of the CSG is to champion** excellence in state governments to advance the common good.

Commercial Vehicle Safety Alliance (CVSA)

Website Link: http://cvsa.org/

The Commercial Vehicle Safety Alliance (CVSA) is a nonprofit association comprised of local, state, provincial, territorial and federal commercial motor vehicle safety officials and industry representatives. The Alliance aims

to achieve uniformity, compatibility and reciprocity of commercial motor vehicle inspections and enforcement by certified inspectors dedicated to driver and vehicle safety. The CVSA mission is to improve commercial motor vehicle safety and uniformity throughout the U.S., Canada and Mexico by providing guidance and education to enforcement, industry and policy makers.

Federal Highway Administration (FHWA)

Website Link: https://www.fhwa.dot.gov/

The Federal Highway Administration (FHWA) is an agency within the U.S. Department of Transportation that supports State and local governments in the design, construction, and maintenance of the Nation's highway system (Federal Aid Highway Program) and various federally and tribal owned lands (Federal Lands Highway Program). Through financial and technical assistance to State and local governments, the Federal Highway Administration is responsible for ensuring that America's roads and highways continue to be among the safest and most technologically sound in the world.

Federal Motor Carrier Safety Administration (FMCSA)

Website Link: https://www.fmcsa.dot.gov/

The Federal Motor Carrier Safety Administration's primary mission is to prevent commercial motor vehicle-related fatalities and injuries. Activities of the Administration contribute to ensuring safety in motor carrier operations through strong enforcement of safety regulations; targeting high-risk carriers and commercial motor vehicle drivers; improving safety information systems and commercial motor vehicle technologies; strengthening commercial motor vehicle equipment and operating standards; and increasing safety awareness. To accomplish these activities, the Administration works with Federal, State, and local enforcement agencies, the motor carrier industry, labor and safety interest groups, and others.

Governors Highway Safety Association (GHSA)

Website Link: www.ghsa.org

GHSA is a nonprofit organization representing the state and territorial highway safety offices that implement federal grant programs to address behavioral highway safety issues. GHSA provides leadership and advocacy for the States and Territories to improve traffic safety, influence national policy, enhance program management and promote best practices.

Institute for Highway Safety (IIHS) and Highway Loss Data Institute (HLDI)

Website Link: http://www.iihs.org/

The Insurance Institute for Highway Safety is an independent, nonprofit scientific and educational organization dedicated to reducing the losses – deaths, injuries and property damage – from crashes on the nation's roads. The Highway Loss Data Institute share and supports the IIHS mission through scientific studies of insurance data representing the human and economic losses resulting from the ownership and operation of different types of vehicles and by publishing insurance loss results by vehicle make and model.

International Association of Chiefs of Police (IACP)

Website Link: http://www.iacp.org/

The International Association of Chiefs of Police (IACP) is a professional association for law enforcement worldwide, representing more than 30,000 members in more than 150 countries. The IACP provides members with the opportunities to connect, participate, learn, advocate, and succeed.

The IACP has divisions, specific sections and policy councils, and committees. Some of these are focused upon traffic safety issues, such as the following:

- **Drug Recognition Expert Section (DRE).** The DRE section provides a unique opportunity for those professionals associated with drug recognition to share common management, training, administrative and practicing concerns.
- **Highway Safety Committee.** This committee studies and evaluates all matters pertaining to policies, practices, and standards of state and municipal policy organizations relating to traffic crash investigation, traffic records, traffic patrol, traffic law enforcement, organization and administration, and other highway safety functions that may be the responsibility of the membership of the IACP. Other key roles include making recommendations for the improvement of police traffic management and the promotion of highway safety; making recommendations to the Traffic Institute of Northwestern University relating to its traffic police training programs; and making recommendations of needed research projects essential to the optimum highway safety programs by police agencies.

  Within the Highway Safety Committee are several Programs and Subcommittees including the:

  - Enforcement Technologies Advisory Technical Subcommittee (ETATS);
  - Traffic Incident Management Subcommittee (TIMS)

- Traffic Officer Safety Subcommittee (TOPS)
- Technical Advisory Panel (TAP)

- **State and Provincial Police Directorate (S&P).** The IACP's Division of State & Provincial Police (S&P) has the responsibility of organizing, directing, coordinating, and promoting IACP programs relating to the needs of state and provincial police agencies. The division is a membership organization comprised of the 49 state law enforcement agencies and three provincial police agencies; the Royal Canadian Mounted Police (RCMP), Ontario Provincial Police, and Sureté du Québec.
- **State and Provincial Police Academy Directors (SPPADS).** SPPADS consists of the commanders and managers of the state and provincial police academies in the United States and Canadian provinces who operate training academies. SPPADS is committed to advancing the principles and competency of professional law enforcement instructors.
- **State and Provincial Police Planning Officers (SPPPOS).** This section consists of planners from the state and provincial agencies, including state police, highway patrols, and departments of public safety, comprising the IACP S&P Directorate. The group meets annually to discuss mutual issues affecting their agencies.
- **State Associations of Chiefs of Police (SACOP).** SACOP serves as the organizing body for the individual state associations of chiefs of police. SACOP also functions as the coordinating body between the state associations and the IACP membership as a whole, facilitating the exchange and dissemination of information related to a host of important topics in law enforcement.
- **Vehicle Crimes Committee.** This committee studies, considers, and determines the various methods and means by which vehicle crimes are committed, including the make and type of vehicles most commonly stolen; surveys, investigates, and evaluates the techniques and methods employed by the police and other agencies in solving and reducing the incidence of vehicle crimes cases; and disseminates pertinent that will reduce the incidence of this major crime.

Institute of Police Technology and Management (IPTM)

Website Link: http://iptm.unf.edu/

Established in 1980, the Institute of Police Technology and Management (IPTM) is a Direct Support Organization (DSO) of the University of North Florida. Headquartered in Jacksonville, Florida, IPTM is a self-supporting, not-for-profit organization. IPTM was created to provide management and traffic training to municipal, county, state, and federal law enforcement officers.

International Association of Directors of Law Enforcement Standards and Training (IADLEST)

Website Link: http://www.iadlest.org.

The International Association of Directors of Law Enforcement Standards and Training (IADLEST) is an international organization of training managers and executives dedicated to the improvement of public safety personnel. IADLEST serves as the national forum of Peace Officer Standards and Training (POST) agencies, boards, and commissions as well as statewide training academies throughout the United States. Within the Association there are specific projects related to traffic safety.

Mothers Against Drunk Drivers (MADD)

Website Link: http://www.madd.org/

Founded by a mother whose daughter was killed by a drunk driver, Mothers Against Drunk Driving® (MADD) is the nation's largest nonprofit working to protect families from drunk driving, drugged driving and underage drinking. MADD also supports drunk and drugged driving victims and survivors at no charge through local MADD victim advocates and a 24-Hour Victim Helpline 1-877-MADD-HELP.

National Conference of State Legislators (NCSL)

Website Link: http://www.ncsl.org/

NCSL is a bipartisan organization that provides state legislators and staffs with independent tools, information and resources to craft the best solutions to challenging problems, including traffic safety issues. The organization promotes policy innovation and communication among state legislatures and ensures representation in the federal system. NCSL has the Standing Committee on Law, Criminal Justice and Public Safety which concentrates on law enforcement and traffic safety concerns.

National District Attorneys Association's National Traffic Law Center (NTLC)

Website Link: http://www.ndaa.org/ntlc_home.html#

The National District Attorneys Association's National Traffic Law Center (NTLC) is a resource designed to benefit prosecutors, judges, law enforcement officers and others in the justice system. The mission of NTLC is to improve the quality of justice in traffic safety adjudications by increasing the awareness of highway safety issues through the compilation, creation and dissemination of legal and technical information, and by providing training and reference services.

National Law Enforcement and Corrections Technology Center (NLETC)

Website Link: https://www.justnet.org/law-enforcement/LE-tech-overview.html

A program of the National Institute of Justice (NIJ), NLETC is the conduit between researchers and criminal justice professionals in the field for technology issues. NLETC works with law enforcement and others to identify urgent and emerging technology needs, test commercially available technologies, and publish results-linking research with practice. NLETC concentrates on law enforcement technology specifically related to traffic safety such as license plate readers, unmanned aircraft systems (UAS) and body-worn cameras.

National Governors' Association (NGA)

Website Link: https://www.nga.org/cms/home.html

This organization consists of the governors of the 50 states, as well as those of the U.S. territories, and the premiers of the Canadian provinces and their top staffs. Members meet periodically to discuss issues of mutual concern among the states, and to support, propose, or endorse legislation in many areas, including criminal laws and highway safety.

National Highway Traffic Safety Administration (NHTSA)

Website Link: https://www.nhtsa.gov/

Through enforcing vehicle performance standards and partnerships with state and local governments, NHTSA reduces deaths, injuries and economic losses from motor vehicle crashes. NHTSA sets and enforces safety performance standards for motor vehicles and equipment, identifying safety defects, and through development and delivery of effective highway safety programs for State and local jurisdictions. NHTSA also has a high-visibility law enforcement effort, coordinated through the Law Enforcement Liaison (LEL) network, which provides effective and efficient delivery of traffic safety countermeasures.

National Organization of Black Law Enforcement Executives (NOBLE)

Website Link: http://www.noblenational.org

The National Organization of Black Law Enforcement Executives (NOBLE) serves as the conscience of law enforcement by being committed to Justice by Action. NOBLE has nearly 60 chapters and represents over 3,000 members worldwide that represent chief executive officers and command-level law enforcement officials from federal, state, county, municipal law enforcement agencies, and criminal justice practitioners. Headquartered in the Washington, D.C., area, NOBLE is comprised of African American command officers in law enforcement agencies.

National Safety Council (NSC)

Website Link: http://www.nsc.org/pages/home.aspx

The National Safety Council eliminates preventable deaths at work, in homes and communities, and on the road through leadership, research, education and advocacy. The NSC provides Defensive Driving Safety Training and Defensive Driving for Emergency Vehicle Operators, among other course offerings.

The National Safety Council also has the Alcohol, Drugs and Impairment Division. This Division tackles substance abuse and prescription drug issues and makes recommendations to combat the drinking and driving problem through legislation, education and other countermeasures. Refer to this website link: http://www.nsc.org/join/Pages/division-alcohol-drugs-and-impairment.aspx

National Sheriffs' Association (NSA)

Website Link: http://www.sheriffs.org/

The National Sheriffs' Association is a professional association dedicated to serving the Office of Sheriff and its affiliates through police education, police training, and general law enforcement information resources. NSA represents thousands of sheriffs, deputies and other law enforcement, public safety professionals, and concerned citizens nationwide. NSA has a Traffic Safety Department serving to perpetuate traffic safety issues, facilitate traffic safety program implementation, provide technical assistance to the office of sheriff and other agencies, and offer general support to the Office of Sheriff and the National Highway Traffic Safety Administration (NHTSA).

Northwestern University Center for Public Safety (NUCPS)

Website Link: https://sps.northwestern.edu/center-for-public-safety/

The Northwestern University Center for Public Safety has a long history of providing educational programs, advocacy and guidance on traffic safety topics. The IACP's Highway Safety Committee and the University have a cooperative partnership promoting excellence in traffic crash investigation, prevention and police management. The Northwestern University Transportation Library has the largest private collection of transportation, highway traffic control, highway safety and criminal justice literature in the United States.

APPENDIX C: ABBREVIATIONS AND ACRONYMS

Abbreviations and Acronyms

The following are some of the more prevalent acronyms used in traffic law enforcement, and their meanings:

ALR/ALS: Administrative License Revocation or Administrative License Suspension. This is referred to in the context of a state statute that permits a police officer to seize a license of a driver who refuses an alcohol test, or tests over the legal alcohol limit. The driver is given a temporary license and scheduled for a prompt administrative hearing before the state driver license agency. ALR/ALS does not replace criminal court action for driving while intoxicated. The purpose of ALR/ALS is to remove the hazard of the drinking driver from the road in a speedier fashion.

AAMVA: The American Association of Motor Vehicle Administrators.

AAMVANET: The American Association of Motor Vehicle Administrators' data services network contains the National Driver Register, Commercial Driver License Information Sys- tem, and other information of interest to licensing, title, regulatory, and law enforcement agencies.

AASHTO: The American Association of State Highway and Transportation Officials.

ABOC: Alcohol Breath Ignition Controller

ADTSEA: American Driver and Traffic Safety Education Association

ALR: Administrative license revocation

ALS: Administrative license suspension

AMA: American Medical Association

AMBER ALERT: A national protocol for the broadcast of in- formation on children who are suspected of having been kid- napped, including posting information about victims and suspects and their vehicles' descriptions on changeable highway warning signs.

BAC: Blood Alcohol Concentration. This is measured in driving- while-intoxicated cases. **BNICE:** A homeland security response describing the five leading threats: **B**iological, **N**uclear/radiological, **I**ncendiary, **C**hemical, and **E**xplosive.

BAIID: Breath Alcohol Ignition Interlock Devices.

BAT: Breath alcohol testing.

BUA: Buckle Up America

BrAC: Breath Alcohol concentration, used in DWI cases and measured in grams per 210 liters of breath (g/210L)

CARE: Combined Accident Reduction Effort. Operation CARE, a group of state police and highway patrol agencies which conduct unified and concentrated efforts in traffic law enforcement along interstate highways, particularly on holiday week- ends.

CDC: Center for Disease Control and Prevention

CDL: A Commercial Driver's License issued by a state entitling a person to operate a commercial motor vehicle which has a manufacturer's gross vehicle weight of 26,001 or more pounds; which is designed to carry 16 or more passengers, including the driver; or which carries hazardous materials. CDL holders in most states are subject to a loss of their CDL if, while driving a commercial vehicle, they have a BAC in excess of 0.04, and are subject to being removed from the road for up to 24 hours if found to have any alcohol in their system while operating a commercial vehicle.

CDLIS: The nationwide Commercial Driver's License Information System contains all commercial driver's license information, including driving histories of problem commercial drivers. It is typically on-line with Motor Carrier Safety Assistance Program (MCSAP) agencies in the various states.

CHEM-TREK: A 24-hour toll-free telephone service that pro- vides law enforcement and emergency response agencies with information for identifying hazardous materials involved in spills, and that recommends mitigation strategies. Chem-Trek is sponsored by the National Chemical Manufacturers' Association.

CLICK-IT-OR-TICKET: A NHTSA program that had its gene- sis in a statewide North Carolina effort and that consists of a concerted, multi-agency safety belt enforcement drive to in- crease safety belt usage through enforcement. Wherever utilized, the program has also resulted in the apprehension of a number of individuals for other serious driving offenses, as well as for criminal offenses, and in the detection of suspended and revoked drivers and persons wanted on criminal warrants.

CVSA: The Commercial Vehicle Safety Alliance.

CPSC: Consumer Product Safety Commission.

CSS: Child Safety Seats.

DARE: Drug Abuse Resistance Education, a copyrighted curriculum. The program, which trains police officers to

present anti- drug programs in public schools, was started by the Los Ange- les Police Department.

DOT: The U.S. Department of Transportation. Also applies to departments of transportation in various states, such as the Arizona Department of Transportation (ADOT) and the Pennsylvania Department of Transportation (PENNDOT).

DRE: A Drug Recognition Expert. Trained and certified in the IACP Drug Evaluation and Classification Program, a DRE is experienced in administering a battery of physical tests and in making clinical observations to suspected drug impaired drivers.

DDMP: Drinking Driver Monitor Program.

DEC: Drug Evaluation and Classification.

DMV: Department of Motor Vehicles.

DUI: Driving under the influence of alcohol or drugs, a criminal offense in most states and provinces. Known as DWI, driving while intoxicated or impaired, in some states.

DWI: Driving while intoxicated; the same as DUI.

DWS: Driving while [license] suspended.

EDR: Event Data Recorder.

EMS: Emergency Medical Services.

ETATS: The Enforcement Technologies Advisory Technical Subcommittee of the IACP's Highway Safety Committee. The Chair of the Highway Safety Committee appoints its members, who include Highway Safety Committee members; persons from the radar, lidar, and automated enforcement industries; a NHTSA representative; technical and scientific ad- visors and representatives of radar certification laboratories. The subcommittee develops standards for the initial testing and ongoing certification of automated enforcement devices such as radar, LIDAR, VASCAR, photo radar, and photo red light running cameras and recommends placement of such de- vices on the CPL (Consumer Products List).

EVOC: Emergency Vehicle Operator's Course. A curriculum developed by NHTSA, in cooperation with national police training professionals, to teach proper techniques for driving police and other emergency response vehicles under emergency conditions.

FARS: The Fatality Analysis Reporting System maintained by the National Highway Traffic Safety Administration (NHTSA). The system gathers data on all fatal traffic crashes in the United States through reports collected by state-level agencies.

FBINA: The Federal Bureau of Investigation's National Academy located at Quantico, Virginia. The academy offers a command training program for high-level officials of state and local law enforcement agencies, and police officials from foreign countries.

FEMA: The Federal Emergency Management Administration, located at Emmitsburg, Maryland, which provides federal emergency assistance at the scenes of catastrophes and national disasters, operates the National Fire Academy, and publishes the national model curriculum for first responders to hazardous materials incidents.

FHWA: The Federal Highway Administration in the U.S. Department of Transportation, which administers federal highway trust fund expenditures to the individual states, and which sets standards for the construction and maintenance of interstate highways.

FMCSA: Federal Motor Carrier Safety Administration, an organizational unit in the U.S. Department of Transportation, the mission of which is to prevent commercial vehicle related fatalities and injuries.

FMVSS: Federal Motor Vehicle Safety Standards as developed and adopted by the National Highway Traffic Safety Administration.

FOP: The Fraternal Order of Police, a national police organization sometimes involved in labor activities as a collective bargaining agent.

FRA: The Federal Railroad Administration, an organizational unit within the U.S. Department of Transportation that monitors the safe operation of railroads. It develops and enforces rail safety regulations, investigates crashes, manages rail safety and highway-rail grade crossing safety programs.

GCCI: Grade Crossing Collision Investigation, a highway-railroad grade crossing safety awareness program, coordinated through a national railroad safety program, Operation Lifesaver. GCCI provides one to three-day training classes, at no cost to the agency, tailored to specific law enforcement agency needs.

GDL: Graduated driver licensing

GHB: Gamma-Hydroxybutyrate. A sedative used both as a prescription sleep-aid and as a recreational intoxicant.

GHSA: The Governors' Highway Safety Association (formerly NAGHSR, the National Association of Governors' Highway Safety Representatives) consists of the Governor's Highway Safety Representative for each state and U.S. Territory and manages the federal pass-through highway safety grants from NHTSA in each state and territory.

HAZMAT: Hazardous materials, generally used in the context of hazardous materials regulatory enforcement.

HGN: Horizontal Gaze Nystagmus, which uses a phenomenon brought on by alcohol and other substances, to assist in deter- mining the blood alcohol level or drug impairment of suspected drunk drivers by examining the angle of onset of nystagmus, a jerking of the eyeballs.

HOS: hours of service

HSC: The Highway Safety Committee of the International Association of Chiefs of Police, Inc., which reports through the IACP's State and Provincial Police Directorate and takes the lead in researching highway and traffic safety issues for the IACP.

HVEE: High-Visibility Education and Enforcement.

IACP: The International Association of Chiefs of Police, Inc.

IACP NET: A password-protected electronic Web site operated by the IACP for its subscriber members. It facilitates the exchange of information and documents between law enforcement agencies throughout the world, at http://www.iacpnet.com

IADLEST: The International Association of Directors of Law Enforcement Standards and Training (POST).

ICS: Incident Command System, the system used by fire departments and police agencies to organize and implement emergency measures to mitigate major incidents.

IFTA: The International Fuel Tax Agreement, a compact consisting of states and provinces that recognize one another's fuel tax laws and providing for one-stop collection and uniform enforcement policies.

IIHS: Insurance Institute for Highway Safety

IMS: Traffic Incident Management System, an adaptation of ICS designed to mitigate the congestion resulting from traffic incidents, to provide prompt treatment of injured persons, and to restore the normal traffic flow as soon as practicable.

IPTM: The Institute of Police Technology and Management at the University of South Florida in Jacksonville, Florida, which conducts law enforcement training programs and which operates a radar testing laboratory.

ITE: The Institute of Transportation Engineers.

ITS: Intelligent Transportation Systems

IVHS: Intelligent Vehicle Highway Systems, a system of computerized hazard detection and warning, trip routing and other capabilities, which interfaces with on-board computers in vehicles equipped with on-board radar and electronic roadside warning beacons.

J. STANNARD BAKER AWARD: An annual award presented by the International Association of the Chiefs of Police and by the National Sheriffs' Association to state, county and local police officers and to private citizens who have made out- standing lifetime contributions to the field of traffic safety. The award is named after the founder of the Traffic Institute at Northwestern University. The IACP's Highway Safety Committee selects the local and state police, as well as the civilian, winners; and the National Sheriffs' Association selects the winners from among County Sheriffs' Offices.

LATCH: Lower Anchors and Tethers for Children.

MADD: Mothers Against Drunk Driving.

MCSAP: The Motor Carrier Safety Assistance Program, a system of federal funding of state agencies to assist the federal Motor Carrier Safety Administration in enforcing motor carrier safety and hazardous materials regulations at the state level.

MDMA: Methylenedioxymethamphetamine. A stimulant drug that is chemically related to mescaline and amphetamine and is used illicitly for its euphoric and hallucinogenic effects

MSF: Motorcycle Safety Foundation

MUTCD: The Manual of Uniform Traffic Control Devices, a publication of the Uniform Traffic Control Devices Committee, that lists and describes the state of the art in traffic sign- age, road markings, traffic lights and other traffic control devices.

MVC: Motor Vehicle Crash (or Collision).

MVOSS: Motor Vehicle Occupant Safety Survey.

NCHRP: National Cooperative Highway Research Program

NDLC: The National Driver License Compact, a program administered by AAMVA in which approximately 43 states participate.

NCSDR: National Center for Sleep Disorders Research

NCUTLO: National Committee on Uniform Traffic Laws and Ordinances

NDR: The National Driver Register, a NHTSA program linked by AAMVANET and maintained by the American Association of Motor Vehicle Administrators.

NHTSA: The National Highway Traffic Safety Administration, an organizational unit of the U.S. Department of Transportation which provides federal

grants to state pass-through agencies for the maintenance of innovative traffic safety programs, conducts research, and sets federal motor vehicle safety standards (FMVSS).

NIAAA: National Institute on Alcohol Abuse and Alcoholism (a branch of National Institutes of Health)

NIH: National Institutes of Health

NIST: The National Institute of Standards and Technology, formerly the National Bureau of Standards.

NMSL: National Maximum Speed Limit.

NRS: National Roadside Survey

NSA: The National Sheriffs' Association.

NSC: The National Safety Council.

NSF: National Sleep Foundation.

NTC: The National Troopers' Coalition.

NTSB: The National Transportation Safety Board, which investigates major transportation crashes and makes recommendations for improved transportation safety.

NUCPS: The Northwestern University Center for Public Safety (formerly the Traffic Institute at Northwestern University) in Evanston, Illinois, which conducts research and offers innovative traffic safety training programs, including courses for commanders of police department traffic bureaus and divisions.

ODPR: Office of Driver and Pedestrian Research.

OL: Operation Lifesaver, a nationwide, nonprofit public information and education program dedicated to reducing crashes, injuries and fatalities at highway-rail grade crossings.

OOT: Officer on the Train, a highway-railroad grade crossing safety awareness program coordinated through a national rail- road safety program, Operation Lifesaver. OOT places police officers aboard trains to radio traffic violations to other officers strategically located at or near grade crossings that have a history of traffic violations.

OPERATION PIPELINE: An enforcement effort along major highway corridors addressing criminal roadway interdiction of passenger and commercial motor vehicles.

OPUE: Occupant Protection Usage and Enforcement. A NHTSA program designed to provide police agencies with a model curriculum and programs to promote and enforce the use of safety belts and child safety seats.

OSHA: The Occupational Safety and Health Administration of the U.S. Department of Labor, which sets standards in many occupational safety areas, including the allowable emissions of police traffic radar devices.

OUI: Operating Under the Influence of Intoxicants.

OUIL: Operating Under the Influence of Liquor, a criminal charge similar to DWI or DUI.

PAS: Passive Alcohol Sensing.

PBT: A Preliminary Breath Test, usually accomplished by means of an electronic fuel cell device, or a balloon-style device that determines at roadside whether or not a driver has consumed alcoholic beverages, and to what extent. Various fuel cell devices have been approved by NHTSA according to standards developed by the IACP Highway Safety Committee's Technical Advisory Panel.

PI&E: Public Information and Education.

PMVI: Periodic Motor Vehicle Inspection, generally a statewide program for the safety inspection of vehicles either at state- owned inspection stations or licensed private stations. The number of states with PMVI has been decreasing over the years.

PSA: Public Service Announcement.

PSU: Primary Sampling Unit.

PTS: Police Traffic Services.

RID: Remove Intoxicated Drivers.

RSP: Ride Service Programs.

RSPA: The Research and Special Programs Administration of the U.S. Department of Transportation, which is responsible for promulgating the provisions of the Code of Federal Regulations pertaining to the transportation of hazardous materials.

SACOP: The State Associations of Chiefs of Police, a division of the IACP, consisting of a designated representative of the Po- lice Chiefs' Association of each state.

SADD: Students Against Driving Drunk.

SAFETYNET: Computerized nationwide data bank maintained by the Motor Carrier Safety Assistance Program for tracking commercial driver enforcement.

SBUL: Safety Belt Use Law.

SFST: Standardized Field Sobriety Testing, a model curriculum developed by the IACP's Highway Safety Committee and NHTSA for performing uniform and standardized roadside physical tests on suspected drunken drivers, based on medically approved techniques. The standardized tests consist of a walk and turn, one-legged stand, and horizontal gaze nystagmus.

STEP: Selective Traffic Enforcement Programs, targeted to the times of day, days of week, locations, and types of violations that cause crashes; an early form of directed patrol, but specifically devised for traffic enforcement.

SHSO: State Highway Safety Office.

TAP: The Technical Advisory Panel of the IACP that, in conjunction with NHTSA, sets and maintains SFST and DRE standards.

TIRF: Traffic Injury Research Foundation.

TITLE 49: Title 49 of the Code of Federal Regulations (CFR), which contains the regulations on the interstate transportation of hazardous materials.

TRB: Transportation Research Board.

TSC: Transportation Systems Center.

USDOT: U.S. Department of Transportation.

UTCD: Uniform Traffic Control Devices Committee, a group of primarily engineers who maintain and revise the National *Manual on Uniform Traffic Control Devices*.

UVC: The *Uniform Vehicle Code*, a model code that is maintained by a standing committee of experts, the National Committee on Uniform Traffic Laws and Ordinances.

VDP: Violator Directed Patrol.

VIN: Vehicle Identification Number

VMT: Vehicle Miles Traveled

APPENDIX D: TRAFFIC SAFETY RESOURCE PROSECUTORS

Alabama
Bill Lindsey
Traffic Safety Resource Prosecutor
515 South Perry St.
Montgomery, AL 36103
Phone: 334.242.4191
Fax: 334.240.3186
Email: william.lindsey@alabamada.gov

Alaska
CURRENTLY VACANT

Arizona
L. Beth Barnes
Assistant City Prosecutor, City of Phoenix
300 West Washington, 8th Floor
Phoenix, Arizona 85003
Phone: 602.262.6461
Email: beth.barnes@phoenix.gov
Web: http://phoenix.gov/LAW/tsrp.html

Arkansas
Mark L. Carpenter
Traffic Safety Resource Prosescutor
Office of the Prosecutor Coordinator
323 Center St, Ste 750
Little Rock, Arkansas 72201
Phone: 501.682.3576
Email: Mark.Carpenter@arkansas.gov

California
Hoon Chang
Traffic Safety Resource Prosecutor
Orange County District Attorneys Office
401 W. Civic Center Drive
Santa Ana, Ca 92701
Phone: 714.347.8620
Email: hoon.chang@da.ocgov.com

Kate Wagner
Traffic Safety Resource Prosecutor
Orange County District Attorneys Office
401 W. Civic Center Drive
Santa Ana, Ca 92701
Phone: 714.347.8883
Email: kate.wagner@da.ocgov.com

Colorado
Jennifer Tibbitts Knudsen
Traffic Safety Resource Prosecutor
Colorado District Attorneys' Council
1580 Logan Street, Suite 420
Denver, CO 80203
Phone: 303.957.2547
Email: jen@cdac.state.co.us
Web: www.cdacweb.com

Connecticut
CURRENTLY VACANT

Delaware
Danielle J. Brennan
Deputy Attorney General
Delaware Department of Justice
820 North French Street, 7th Floor
Wilmington, Delaware 19801
Phone: 302.577.8894
Fax: 302.577.6499
Email: danielle.brennan@state.de.us

District of Columbia
Melissa G. Shear
Assistant Attorney General
Office of the Attorney General
Public Safety Division - Criminal Section
441 4th Street, NW, Suite 1060N
Washington, DC 20001
Phone: 202.724.6633
Fax: 202.730.1478
Email: Melissa.Shear@dc.gov

Florida
Vincent Petty
Traffic Safety Resource Prosecutor
Unit 107 PMB 108
14851 State Road 52
Hudson, FL 34669-4061
Phone: 850-566-9021
Email: VinPetty@FloridaTSRP.com

Georgia
Gilbert A. Crosby
Prosecuting Attorneys' Council of Georgia
104 Marietta, Suite 400
Atlanta, GA 30303-2743
Phone: 404.969.4001
Fax: 404.969.4020
Email: gcrosby@pacga.org

Hawaii
Stephen L. Frye
Deputy Prosecuting Attorney
Office of the Prosecuting Attorney – County of Hawaii
81-980 Haleki'i St., Suite #150
Kealakekua, HI 96750
Phone: 808-322-2552
Fax: 808-322-6584
Email: Stephen.Frye@HawaiiCounty.gov

Ramsey Ross
Deputy Prosecuting Attorney-County of Kaua'i
3990 Ka'ana Road
Lihue, Kaua'i 96766
Phone: 808-241-1911
Email: rross@kauai.gov

Idaho
Jared Olson
Idaho Prosecuting Attorneys Association
Idaho POST Academy
700 S. Stratford Drive
Meridian, ID 83642
Phone: 208.884.7325
Fax: 208.884.7295
Cell: 208.559.1217
Email: Jared.olson@post.idaho.gov
Web: www.TSRP-Idaho.org

Illinois
Jennifer L. Cifaldi
Illinois Traffic Safety Resource Prosecutor
Institute For Legal, Legislative and
Policy Studies
Univ. of Illinois Springfield, Center for State
Policy and Leadership
One University Plaza, MS PAC 451
Springfield, Illinois 62703-5407
Phone: (217) 257-5050
Email: jcifaldi3@gmail.com

Indiana
Christopher Daniels
Indiana Prosecuting Attorneys Council
302 W. Washington Street, E-205
Indianapolis, IN 46204-2767
Phone: 317.232.1836
Fax: 317.233.3599
Email: chdaniels@ipac.in.gov

Iowa
Christine Shockey
Assistant Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
Phone: 515.281.5428
Email: Christine.shockey@iowa.gov

Kansas
Corey Kenney
Assistant Attorney General - Traffic Safety
Resource Prosecutor
Office of Kansas Attorney General Derek Schmidt
120 SW 10th Avenue, 2nd Floor
Topeka, KS 66612
Office: (785) 296-3750
Fax: (785) 291-3875
Email: Corey.Kenney@ag.ks.gov

Kentucky
Bob Stokes
Traffic Safety Resource Prosecutor
1024 Capital Center Drive, Suite 200
Frankfort, KY 40601
Phone: 502.696.5500
Fax: 502.696.5532
Email: bstokes@prosecutors.ky.gov
Web: www.kytrafficsafety.com

Louisiana
Rachel Smith
Louisiana District Attorneys Association
1645 Nicholson Drive
Baton Rouge, LA 70802-8143
Phone: 225.343.0171
Fax: 225.387.0237
Email: Rachel@LDAA.org

Maine
Scot Mattox
Traffic Safety Resource Prosecutor
45 Commerce Drive, Suite 1
164 State House Station
Augusta, ME 04333-0164
Phone: 207.458.0913
Email: Scot.Mattox@maine.gov

Maryland
David Daggett
Maryland State's Attorneys Association
3300 North Ridge Road, Ste 185
Ellicott City, MD 21043
Phone: 410.203.9881
Cell: 410.979.3356
Email: ddaggett@mdsaa.org

Massachusetts
Andrea Nardone
Mass. District Attorneys Association
1 Bulfinch Place, Suite 202
Boston, MA 02114
Phone: 617.723.0642
Fax: 617.367.1228
Email: Andrea.Nardone@state.ma.us
Web: www.mass.gov/mdaa

Michigan
Ken Stecker
Traffic Safety Resource Prosecutor
Prosecuting Attorneys Association of Michigan
116 West Ottawa, Suite 200
Lansing, MI 48913
Phone: 517.334.6060 ext 827
Fax: 517.334.7052
Email: steckerk@michigan.gov
Web: https://www.michiganprosecutor.org/

Kinga Gorzelewski
Traffic Safety Resource Prosecutor
Prosecuting Attorneys Association of Michigan
116 West Ottawa, Suite 200
Lansing, MI 48913
Phone: 517.334.6060 ext 816
Fax: 517.334.7052
Email: gorzelewskik@michigan.gov
Web: https://www.michiganprosecutor.org/

Minnesota
Bill Lemons
Minnesota County Attorney Association
100 Empire Drive, Suite 200
St. Paul, MN 55103
Phone: 651. 289.8451
Email: blemons@mcaa-mn.org
Web: www.mcaa-mn.org

Mississippi
Molly Miller
Mississippi Attorney General's Office
Walter Sillers Bldg.
550 High Street, P.O. Box 220
Jackson, MS 39205
Phone: 601.359.4265
Fax: 601.359.4200
Email: mmill@ago.state.ms.us

Missouri
Susan Glass
Missouri Office of Prosecution Services
P.O. Box 899
Jefferson City, MO 65102
Phone: 573.301.2630
Fax: 573.751.1171
Email: Susan.Glass@prosecutors.mo.gov

Stephanie Watson
Missouri Office of Prosecution Services
P.O. Box 899
Jefferson City, MO 65102
Phone: 573.751.2415
Fax: 573.751.1171
Email: Stephanie.Watson@prosecutors.mo.gov

Montana
CURRENTLY VACANT

Nebraska
Ed Vierk
Attorney General's Office
2115 State Capital
Lincoln, NE 68509
Phone: 402.471.1886
Fax: 402.471.3591
Email: Ed.Vierk@nebraska.gov

Nevada
Bruce Nelson
Deputy District Attorney
200 Lewis Ave
Box 552212
Las Vegas, NV 89155-2212
Phone: 702.671.2807
Email: bruce.nelson@clarkcountyda.com

Chris Halsor
Traffic Safety Resource Prosecutor
Office of the Attorney General
100 N. Carson Street
Carson City, NV 89701-4717
Phone: 775 430-0322
Email: chris.halsor@ag.nv.gov.

New Hampshire
Scott Chase
Traffic Safety Resource Prosecutor Criminal Justice Bureau Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Phone: 603 271 3685
Fax: 603 271 2110
Email: scott.chase@doj.nh.gov

New Jersey
Robyn Mitchell
Division of Criminal Justice
25 Market Street
PO Box 086
Trenton, NJ 08625-0086
Phone: 609.777-0246
Fax: 609.341.2077
Email: mitchellr@njdcj.org

Erin Shamy
Deputy Attorney General
Division of Criminal Justice
25 Market St.
P.O. Box 085
Trenton, NJ 08625-0085
Phone: 609.984.4776
Email: shamye@njdcj.org

New Mexico
Aaron Baca
Traffic Safety Resource Prosecutor
New Mexico Attorney General's Office
Special Prosecutions Division
408 Galisteo Street
Santa Fe, New Mexico 87501
Phone: 505.827.6064
Email: abaca@nmag.gov

New York
Lauren D. Konsul
New York Prosecutors Training Institute
107 Columbia Street
Albany, NY 12210
Phone: 518.432.1100 x. 203
Fax: 518.432.1180
Email: lauren.konsul@nypti.org
Web: www.nypti.org

North Carolina
Isaac T. Avery, III
The Avery, P.C.
P. O. Box 10174
Raleigh, NC 27605-0174
Phone: 919.829.2523
Fax: 919.834.9812
Email: isaac.t.avery@aoc.nccourts.org

Sarah Z. Garner
NC Conference of District Attorneys
P. O. Box 3159
Cary, NC 27519
Phone: 919.890.1500
Fax: 910.641.4502
Email: Sarah.z.garner@nccourts.org

North Dakota
Aaron Birst
1661 Capitol Way
P.O. Box 877
Bismarck, North Dakota 58502-0877
Phone: 701.328.7342
Fax: 701.328.7308
Email: aaron.birst@ndaco.org

Kristi Pettit Venhuizen
311 South 4th Street, Suite 103
Grand Forks, ND 58201
Phone: 701.780.9276
Fax: 701.780.0786
Email: kpettit@kalashpettitlaw.com

Ohio
Holly Reese
Traffic Safety Resource Prosecutor
Ohio Traffic Safety Office
c/o Stark County Sheriff's Office
4500 Atlantic Blvd., N.E.
Canton, Ohio 44705
Phone: 330.904.8971
Email: hreesetsrp@gmail.com

Oklahoma
Jeff Sifers
District Attorneys Council
421 N.W. 13th Street, Ste 290
Oklahoma City, OK 73103
Phone: 405.264.5000
Fax: 405.264.5099
E-mail: jeff.sifers@dac.state.ok.us

Oregon
Deena Ryerson
Oregon District Attorneys Association
610 Hawthorne Ave Ste. 210
Salem, Oregon 97301
Phone: 503.378.6347
Email: Deena.a.ryerson@doj.state.or.us

Amy Seely
Assistant Attorney General, DUII Resource Prosecutor
Oregon Department of Justice
2250 McGilchrist St. SE, Salem, OR 97302
Office: 503.934.2082
Cell: 503.871.9608
Email: amy.seely@doj.state.or.us

Pennsylvania
Dave Drumheller
Pennsylvania District Attorneys Association
2929 North Front Street
Harrisburg, PA 17110
Phone: 717. 238.5416
Email: ddrumheller@pdaa.org
Web: www.pdaa.org

Rhode Island
John Corrigan
Assistant Attorney General RI Attorney General
150 South Main Street Providence, RI 02903
Phone: (410) 274-4400 ext 2009
E-mail: jcorrigan@riag.ri.gov

South Carolina
Mattison Gamble
Traffic Safety Resource Prosecutor
S.C. Common Prosecution Coordination
P. O. Box 11561
Columbia, SC 29211
Phone: 803.343.0765
Fax: 803.343.0766
Email: mgamble@cpc.sc.gov

South Dakota
Paul Bachand
PO Box 1174
Pierre, SD 57501-1174
Phone: 605.224.0461
Email: pbachand@pirlaw.com

Tennessee
Barry Williams
Tenn. District Attorneys General Conf.
226 Capitol Blvd., Suite 800
Nashville, TN 37243-0890
Phone: 615.945.2040
Fax: 615.741.7459
Email: bawilliams@tndagc.org
Web: www.dui.tndagc.org
Blog: http://tnduiguy.blogspot.com/

Terry Wood
Tenn. District Attorneys General Conf.
226 Capitol Blvd., Suite 800
Nashville, TN 37243-0890
Phone: 615 253 6734
Email: tewood@tndagc.org
Web: www.dui.tndagc.org
Blog: http://tnduiguy.blogspot.com/

Texas
W. Clay Abbott
Texas District & County
Attorneys Association
505 W. 12th, Suite 100
Austin TX, 78701
Phone: 512.474.2436
Email: Clay.Abbott@tdcaa.com
Web: www.tdcaa.com

Utah
Tyson K. Skeen
Traffic Safety Resource Prosecutor
Utah Prosecution Council
P.O. Box 140841
Salt Lake City, UT 84114-0841
Phone: 801.366.0334
Cell: 801.391.9667
Email: tskeen@utah.gov

Vermont
Heather J. Brochu
Traffic Safety Resource Prosecutor
Dept of State's Attorneys and Sheriffs
110 State Street
Montpelier, Vt 05633-6401
Phone: 802 828 2891
Fax: 802 828 2881
Email: heather.brochu@vermont.gov

Virginia
Walter E. Hibbard
Traffic Safety Resource Prosecutor
Commonwealth's Attorneys' Services Council
P.O. Box 3549
Williamsburg, VA 23187-3549
Phone: 757.253.4994
Email: whibbard@wm.edu
Web: www.cas.state.va.us

John C. Bowers
Traffic Safety Resource Prosecutor
Commonwealth's Attorneys' Services Council
P.O. Box 3549
Williamsburg, VA 23187-3549
Phone: 757.746.5653
Email: jcbowers@wm.edu
Web: www.cas.state.va.us

Washington
Moses F. Garcia
Traffic Safety Resource Prosecutor
MRSC
2601 Fourth Ave., Suite 800
Seattle, WA 98121-1280
Phone: 206.625.1300
Email: mgarcia@mrsc.org

Courtney Popp
Traffic Safety Resource Prosecutor
King County Sheriff's Office
ATTN: CID ATU
500 4th Ave., Suite 200
Seattle, WA 98104
Phone: 206-743-7772
Email: Courtney.popp@kingcounty.gov

Miriam Norman
Traffic Safety Resource Prosecutor
701 Fifth Avenue, Suite 2050
Seattle, WA 98104-7097
Phone: 206-684-8526
Cell: 206-850-5260
Fax: 206-684-4648
Email: miriam.norman@seattle.gov

Katie McNutly
Traffic Safety Resource Prosecutor
Spokane County Prosecutor's Office
Spokane, WA 99260-0270
Phone: 509 477 3662
Email: kmcnulty@spokanecounty.org

West Virginia
Nicole Cofer-Fleming
Traffic Safety Resource Prosecutor
Kanawha County Prosecuting Attorney's Office
301 Virginia St. E
Charleston, WV 25301
Phone: 304-357-5143
Fax: 304-357-0342
Email: ncofer@kanawhaprosecutor.com

Wisconsin
Tara Jenswold
Traffic Safety Resource Prosecutor
Assistant Attorney General
Wisconsin Department of Justice
17 W. Main Street
Madison, WI 53707
Phone: 608.266.8908
Fax: 608.267.2778
Email: jenswtm@doj.state.wi.us

Wisconsin (cont'd.)
Emily Thompson
Traffic Safety Resource Prosecutor
Assistant Attorney General
Wisconsin Department of Justice
17 W. Main Street
Madison, WI 53707
Phone: 608.266.8941
Fax: 608.267.2778
Email: thompsonel@doj.state.wi.us

Wyoming
Ashley C. Schluck
Wyoming Traffic Safety Resource Prosecutor
Wyoming Highway Safety Program
P.O. Box C
Laramie, WY 82073
Phone: 307.721.5321
Fax: 307.721.5318
Email: acastor@cityoflaramie.org

National Traffic Law Center
Joanne Thomka
Director, National Traffic Law Center
National District Attorneys Association
1400 Crystal Drive, Suite 330
Arlington, VA 22202
Phone: 703.519.1678
Fax: 703.836.3195
Email: jthomka@ndaajustice.org
Web: www.ndaajustice.org

M. Kimberly Brown
Senior Attorney, NTLC
National District Attorneys Association
1400 Crystal Drive, Suite 330
Arlington, VA 22202
Phone: 703.519.1645
Fax: 703.836.3195
Email: mkbrown@ndaajustice.org
Web: www.ndaajustice.org

Romana Lavalas (Commercial Motor Vehicles)
Senior Attorney, NTLC
1400 Crystal Drive Suite 330
Arlington, Va 22202
Phone: 703.519.1674
Fax: 703.836.319
Email: rlavalas@ndaajustice.org
Web: www.ndaajustice.org

Stacey Grant (Commercial Motor Vehicles)
Staff Attorney, NTLC (part time)
National District Attorneys Association
1400 Crystal Drive, Suite 330
Arlington, VA 22202
Phone: 703.519.1644
Fax: 703.836.319
Email: sgrant@ndaajustice.org
Web: www.ndaajustice.org

Sam Pellegrino
Staff Attorney, NTLC
National District Attorneys Association
1400 Crystal Drive, Suite 330
Arlington, VA 22202
Phone: 703.519.1642
Fax: 703.836.3195
Email: spellegrino@ndaajustice.org
Web: www.ndaajustice.org

Peter Grady
Senior Attorney, NTLC (part time)
1400 Crystal Drive, Suite 330
Arlington, Va 22202
Email: pgrady@ntlc.org

Metria Hernandez
Senior Project Coordinator
National District Attorneys Association
1400 Crystal Drive, Suite 330
Arlington, VA 22202
Phone: 703.519.1683
Fax: 703.836.3195
Email: mhernandez@ndaajustice.org
Web: www.ndaajustice.org

NAPC Program
Thomas M. Robertson
Executive Director
8283 Williams Road
Dewitt, MI 48820
Phone: 517-402-8177
Email: Trob@napc.us
Web: http://www.napc.us/

ACKNOWLEDGEMENTS

This project was funded by the National Highway Traffic Safety Administration (NHTSA). The support and contributions of the NHTSA staff were instrumental in the final product. The IACP would like to thank NHTSA for providing this resource to law enforcement officers – the front line leaders making an impact on traffic safety, every hour of every day. Specifically, Keith Williams, NHTSA Division Chief, and Wil Price, NHTSA Highway Safety Specialist, provided timely guidance and leadership to the project team.

The IACP would also like to acknowledge the many contributors to the Traffic Safety Resource Guide. Noteworthy assistance was provided by the members of the IACP Highway Safety Committee whose support was invaluable in completing the project. Under the leadership of Commissioner Joseph Farrow, formerly with the California Highway Patrol and now the Chief of Police at the University of California at Davis, the project team was able to consult with the Highway Safety Committee and draw upon the considerable experience of the Committee.

The project commenced with the formation of a Traffic Safety Resource Guide Committee. This dedicated group worked tirelessly on a variety of tasks including project management, writing, editing, and ensuring the final product met the high standards embraced by all law enforcement leaders. The following individuals served as members of this Committee:

Vernon F. Betkey, Jr.
National Law Enforcement Liaison Program Manager
Governors Highway Safety Association

M. Kimberly Brown
National Traffic Law Center, National District Attorneys Association - Virginia

Captain Arthur Combest
Ohio State Highway Patrol

Captain Thomas Didone
Montgomery County, Maryland, Police Department

Ed Hutchison
National Sheriffs Association

Annjanette Kremer, P.E.
Michigan Department of Transportation

Staff Sergeant Terence J. McDonnell
New York State Police
Lieutenant Matt Myers
Peachtree City, Georgia, Police Department

Wil Price
National Highway Traffic Safety Administration

Jack Van Steenburg
Federal Motor Carrier Safety Administration

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE EXECUTIVE STAFF

Vincent Talucci
Executive Director/CEO

Terrence Cunningham
Deputy Executive Director

Domingo Herraiz
Director, Programs

PROJECT STAFF

Mike Fergus
Project Director, Programs

Samuel Capogrossi,
Project Manager, Programs

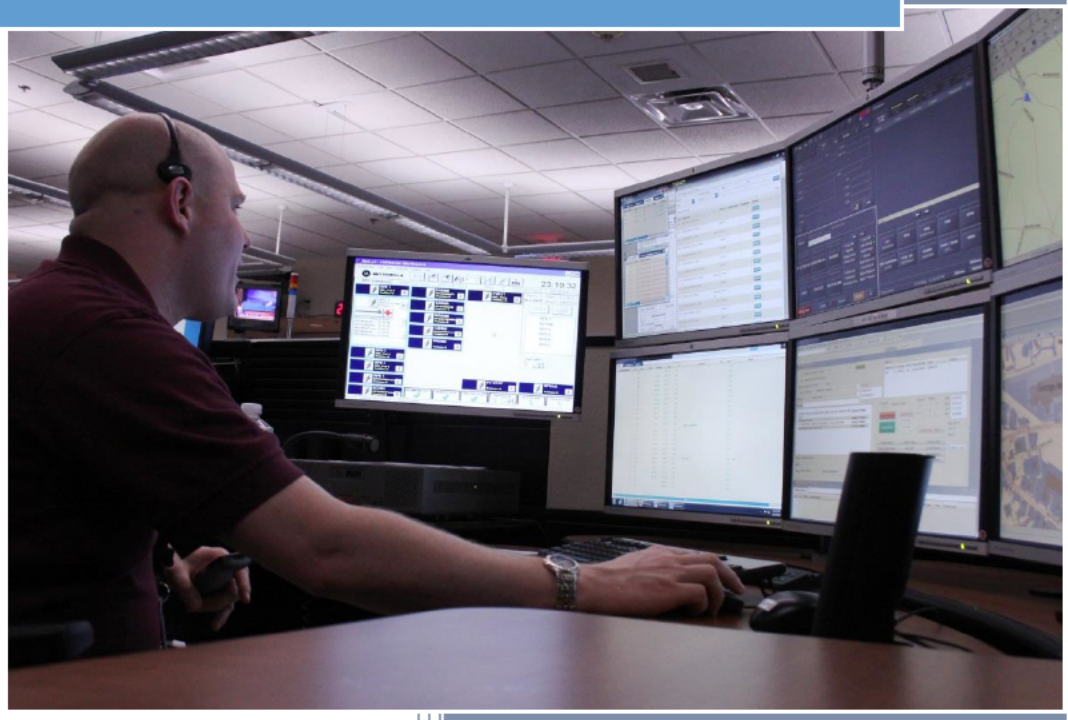
Bethany Peterson
Project Coordinator, Programs

Mark W. Seifert
Traffic Safety Resource Guide, Project Manager

APCO International
Leaders in Public Safety Communications™

IJIS Institute

UNIFIED CAD FUNCTIONAL REQUIREMENTS



APCO International

IJIS Institute

UCAD Project Committee

Functional Requirements

August 2012

This project was supported by Grant No. **2010-DB-BX-K147** awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

ACKNOWLEDGEMENTS

We would like to offer our sincere thanks to the following persons for their time and effort provided to bring this document to completion:

TABLE 1. ACKNOWLEDGEMENTS

UCAD PROJECT COMMITTEE	**Evan Bestland**	*Division Chief, ITS*	Palm Beach County Fire Rescue (FL)
	Donald Bowers	*Battalion Chief*	Fairfax County Fire & Rescue Department (VA)
	Bret Crook	*Captain*	Woodway Public Safety Department, (TX)
	James W. Dundas	*Business Development Manager*	Northrop Grumman Information Systems
	Peggy Fouts	*Director*	Grays Harbor Communications E9-1-1 (WA)
	Karen E. Jacobson	*NEMSIS Director*	University of Utah School of Medicine (UT)
	Chris Kummer	*Manager - Communications*	Hennepin Emergency Medical Services (MN)
	Norine Plett	*Lieutenant*	Los Angeles County Sheriff's Office (CA)
	David Roberts	*Senior Program Manager, State and Provincial Police Division*	IACP Technology Center
	Mike Roosa	*CIO*	Maryland State Police (MD)
	Jerry Schlesinger	*RegJIN RMS Project Manager*	City of Portland, Public Safety Systems Revitalization Program (PSSRP) (OR)
	Matt Schreiner	*PremierOne CAD Product Manager*	Motorola
	Daniel Stilwell	*Senior Dispatcher*	Seattle Fire Department, Communications Division (WA)
	Lance Terry	*Communication Systems Manager*	City of Norman (OK)
	Henry Unger	*President*	Hitech Systems, Inc.
	Dennis C. Wood	*Major*	Prince George's County Fire/EMS Department (MD)
PROJECT MANAGEMENT TEAM	**Bill Hobgood**	*Project Coordinator*	Association for Public-Safety Communications Officials International (APCO)
	Paul Holcombe	*Project Manager*	IJIS Institute
	Randy Kent	*Project Manager*	IJIS Institute
	Scott Parker	*Program Manager*	IJIS Institute
	Chris Traver	*Senior Policy Advisor*	Bureau of Justice Assistance (BJA)*
	Stephen Wisely	*Director*	Association for Public-Safety Communications Officials International (APCO)
SUBCONTRACTOR	**Tom Maureau**	*Project Manager & SME*	Winbourne & Costas, Inc.

* Special appreciation is extended to the Bureau of Justice Assistance for its support to the justice and public safety communities. This project is one of many activities where the BJA has demonstrated its commitment to cross-boundary collaboration and partnership with the public safety community as a whole by bridging information sharing gaps between traditional justice agencies and first responders.

Cover Photo Credit

- *Photographer*: Joel Klein
- *Supplied by*: City Of Richmond, Virginia

To ensure that the final version of this paper adequately addressed CAD functionality requirements for law enforcement, fire and Emergency Medical Service (EMS), the UCAD Project Committee reached out to a number of organizations within the stakeholder communities and requested feedback on the *UCADFR* draft. The UCAD Project Committee would like to thank the following organizations for their many thoughtful comments and excellent suggestions on this document:

- American Ambulance Association (AAA)
- Association of Public-Safety Communications Officials International (APCO)
- City of Westminster, Colorado
- IJIS Institute, Public Safety Technology Standards Committee (IPSTSC)
- Institute for Intergovernmental Research (IIR)
- International Association of EMS Chiefs (IAEMSC)
- International Association of Fire Chiefs (IAFC)
- International Association of Fire Fighters (IAFF)
- National Fire Information Council (NFIC)
- SEARCH, The National Consortium for Justice Information and Statistics

TABLE OF CONTENTS

ACKNOWLEDGEMENTS ..... **III**

TABLE OF CONTENTS ..... **V**

1 INTRODUCTION **1**

1.1 CAD Systems 1
1.2 Background 4
1.3 Notes to the Reader 5
1.4 Using This Document for RFP Creation 10
1.5 UCADFR as a Standard 11

2 CALL HANDLING / CAD EVENT CREATION **12**

2.1 Call Handling 12
2.2 CAD Incident / Event Types 13
2.3 Update Call for Service Event Data 15
2.4 Determine Dispatch Need 16
2.5 Utilize Incident Disposition 17
2.6 Assign Incident Classification and Priority 18
2.7 Check for Duplicate Incidents 19
2.8 Incident Information 21
2.9 Determining Capture Locations 22
2.10 Location Verification 24
2.11 Retrieve Incoming Calls 26
2.12 Involved Person Information 27
2.13 Involved Vehicle Information 29
2.14 Premises Hazards and Previous History 30
2.15 CAD Event Creation 32
2.16 Determining Response Agency and Service Area 32
2.17 Alarm Processing 34
2.18 CAD Event Routing 35
2.19 Ability to Route to a “Decision Dispatcher” 36

3 DISPATCH SUPPORT **37**

3.1 Run Cards / Response Plans 37
3.2 Adjustable Dispatch Levels 38
3.3 Additional Attributes 39
3.4 Mutual Aid Function 40
3.5 Automatic Aid Function 41
3.6 Unit Rotation (Unit Load Balancing) 42
3.7 Conditional Availability of Apparatus 43
3.8 Special Dispatch Areas 44
3.9 Emergency Medical Dispatch / Incident Triage 45
3.10 Channel Designations 45
3.11 Be On the Look-Out / Attempt to Locate 47
3.12 Dispatch Units 48
3.13 Resource Alerting 48

4 RESOURCE / UNIT MANAGEMENT 51
4.1 Move Up ("Fill-In" and "Station Fill") 51
4.2 Staffed vs. Unstaffed Units 51
4.3 Cross-Staffing / Crew Counting / Shared Staffing / Contingent Staffing 52
4.4 System Status Management (Dynamic Resource Deployment) 53
4.5 Additional Unit Status 54
4.6 Strike Team / Task Force Designations 55
4.7 Rostering 55
4.8 Scheduling 56
4.9 Mileage Tracking 57
4.10 Hydrant Location and Status 57
4.11 Additional Unit Dispositions 58
4.12 Exception Reason Tracking 59
4.13 Public Safety Flight Tracking 59
4.14 Geo-fencing 60
4.15 Station Dispatch 60
4.16 Pre-Release or Pre-Alerting 61
4.17 Vehicle / Unit Change 61
4.18 Automatic Driving Directions / Routing 62
4.19 Bypassed Units 63
4.20 Post-Dispatch Response Re-evaluation 63

5 CALL / INCIDENT / EVENT MANAGEMENT 65
5.1 Display of Incident / Event Data 65
5.2 Update Incident Status 66
5.3 Dispatch Resource Decision 66
5.4 Update Assigned Resources 67
5.5 Update Supplemental Resources Tracking 67
5.6 Assign Units 68
5.7 Update Incident Data 69
5.8 Assign Records Management System Incident / Case Number 70
5.9 Transfer Basic Incident Data to the Records Management System 71
5.10 Display Additional Incident Data 72
5.11 Reopen Incident 73
5.12 Add Destination Locations 73
5.13 Hospital Status / Availability and Hospital Recommendation 74
5.14 Patient Tracking 75
5.15 Linking an Audio File to a CAD Event 76
5.16 Multiple Simultaneous Incidents to Single Unit 77
5.17 Scheduled Events 78
5.18 Secondary Incident Location 79
5.19 Single Discipline Incident to a Combined Discipline Incident 79
5.20 Timers 80
5.21 User Defined Status Timers 81

6 SUPPLEMENTAL RESOURCE REQUEST AND TRACKING 82
6.1 Request Supplemental Resource 82
6.2 Request Supplemental Resource Rotation List 83
6.3 Notify Supplemental Resource Service 83

6.4 Enter and Update Supplemental Service Record 84

7 INCIDENT DISPOSITION 85

7.1 Determine Incident / Event Status 85
7.2 Utilize Incident Management 86
7.3 Determine Report Functionality 86
7.4 Record Disposition 87
7.5 Send Data to Records Management System 87
7.6 Assign Agency-Specific Report Numbers 88

8 BUSINESS FUNCTION: CAD SYSTEM ADMINISTRATION 89

8.1 Geofile Maintenance 90
8.2 Security 94
8.3 Logging 96
8.4 Configuration 97
8.5 Table Maintenance 99
8.6 Communication Center / PSAP Relocation 101
8.7 CAD Catch-Up 101

9 SYSTEM FUNCTIONS 103

9.1 Notifications 103
9.2 Contact List 104
9.3 Premises Information / Hazards 104
9.4 Communications Center / Public Safety Answering Point Standard Operating Procedures 106
9.5 Agency-Specific Incident / Location / Unit Standard Operating Procedures 107
9.6 Remote Access 107
9.7 CAD Workstation-to-CAD Workstation Messaging 108
9.8 Incident Command Support 108
9.9 Narrative Field “Shorthand” / Auto Text 109
9.10 Command Line / GUI 109
9.11 Date/Time Stamps 110
9.12 Unit Status Transitions Matrix 110
9.13 Single Sign-on for CAD and CAD Sub-systems 111
9.14 Multi-Agency / Multi-Jurisdictional Capability 111

10 REPORTING & MONITORING 113

10.1 Dispatch Supervisor Support 113
10.2 CAD Management Reporting 114
10.3 Training and Testing 115
10.4 Snapshot / Incident Replay 116

11 INTERFACES 118

11.1 Essential Interfaces 119
11.2 Additional Interfaces 123
11.3 Locational Systems Interfaces 126
11.4 Administration Interfaces 130
11.5 Communications Interfaces 131
11.6 Integration / Interfaces with Other Systems 132
11.7 National SAR Initiative Functionality 134

11.8 Emergency Operations Center Interface 137

12 FUTURE PIPELINE / ON THE HORIZON 139

12.1 Next Generation 9-1-1 139
12.2 Broadband / Long-Term Evolution 142

13 MOBILE CAD FUNCTIONS 144

14 APPENDICES 145

14.1 APPENDIX A – Related Standards Development Organizations (SDO) 145
14.2 APPENDIX B – Related Models and Standards 145
14.3 APPENDIX C – Global Resources 145
14.4 APPENDIX C – Other Resources 146
14.5 APPENDIX D – Previous Versions of CAD Functional Standards / Requirements 146
14.6 APPENDIX E – Relevancy Matrix 146
14.7 APPENDIX F – Acronyms and Abbreviations 149

LIST OF FIGURES

Figure 1. Public Safety System Integration Framework 3
Figure 2. CAD System Functional Components 4
Figure 3. Typical CAD Geofile 92
Figure 4. Networking with Additional Interfaces 124
Figure 5. Defined Criminal Activity and Potential Terrorism Nexus Activity 135
Figure 6. Notional SAR Process 136
Figure 7. SIP and EIDD Exchanges for Public Safety 140

LIST OF TABLES

Table 1. Acknowledgements iii
Table 2. Location Formats 24
Table 3. Unit Status Modifiers 54

1 INTRODUCTION

The purpose of this document, how the document can be used, its target audience, a basic description of Computer Aided Dispatch (CAD)[1] systems, background regarding the development of this report, and several important notes to the reader are conveyed below.

Purpose of the UCADFR Document

The *Unified CAD Functional Requirements* (*UCADFR*) is an expanded version of the *Standard Functional Specifications for Law Enforcement Computer-Aided Dispatch Systems*, published in 2006 by the Law Enforcement Information Technology Standards Council (LEITSC). The Association for Public Safety Communications Officials (APCO) and the IJIS Institute have noted that the majority of emergency communications centers dispatch for multiple first responder services: a combination of law enforcement, fire, and EMS. Increasingly, localities are seeking to consolidate their communications centers, and this increases the demand for unified CAD systems that serve multiple domains. The *UCADFR* is an invaluable resource to these communities, supporting the planning, acquisition, and management of full-featured CAD software applications.

Public safety stakeholder disciplines also include emergency communications, law enforcement, fire service, EMS, and the CAD provider industry. Practitioners writing Request for Proposals (RFPs) for CAD systems to support multi-service dispatch centers will also benefit from this document.

Use of the UCADFR Document

The *UCADFR* includes a detailed, comprehensive, and unified set of functional requirements for CAD systems. Each CAD function is identified with a visual flag to indicate what service(s) (whether law enforcement, fire, or EMS) the function applies to. Sample requirements for each function are provided and can be incorporated in an RFP when a public safety communications center has a need to conduct a solicitation for a new CAD system.

Target Audience

This document is targeted to individuals within organizations having a stake in CAD functional specifications. It is assumed that the reader has knowledge of CAD, its purpose, and its use.

1.1 CAD Systems

A *CAD system* is the principal application used by public safety agencies to manage law enforcement, fire, and EMS incidents from the initial time an incident is reported to the conclusion of the incident. CAD is also used to track the status and location of resources, and for post-incident analysis of the response.

A CAD system consists of either a single software application or a suite of integrated software packages used to initiate a public safety call for service (CFS) record, to dispatch, to maintain the status of responding units and resources in the field, and to generally manage the incident. It is typically used by emergency communications dispatchers, call takers, and telecommunicators in public-safety communications centers. Modern CAD systems are usually extended out to field personnel (responders)

[1] See Section 14.6: APPENDIX F for a full list of all acronyms and abbreviations used in this document.

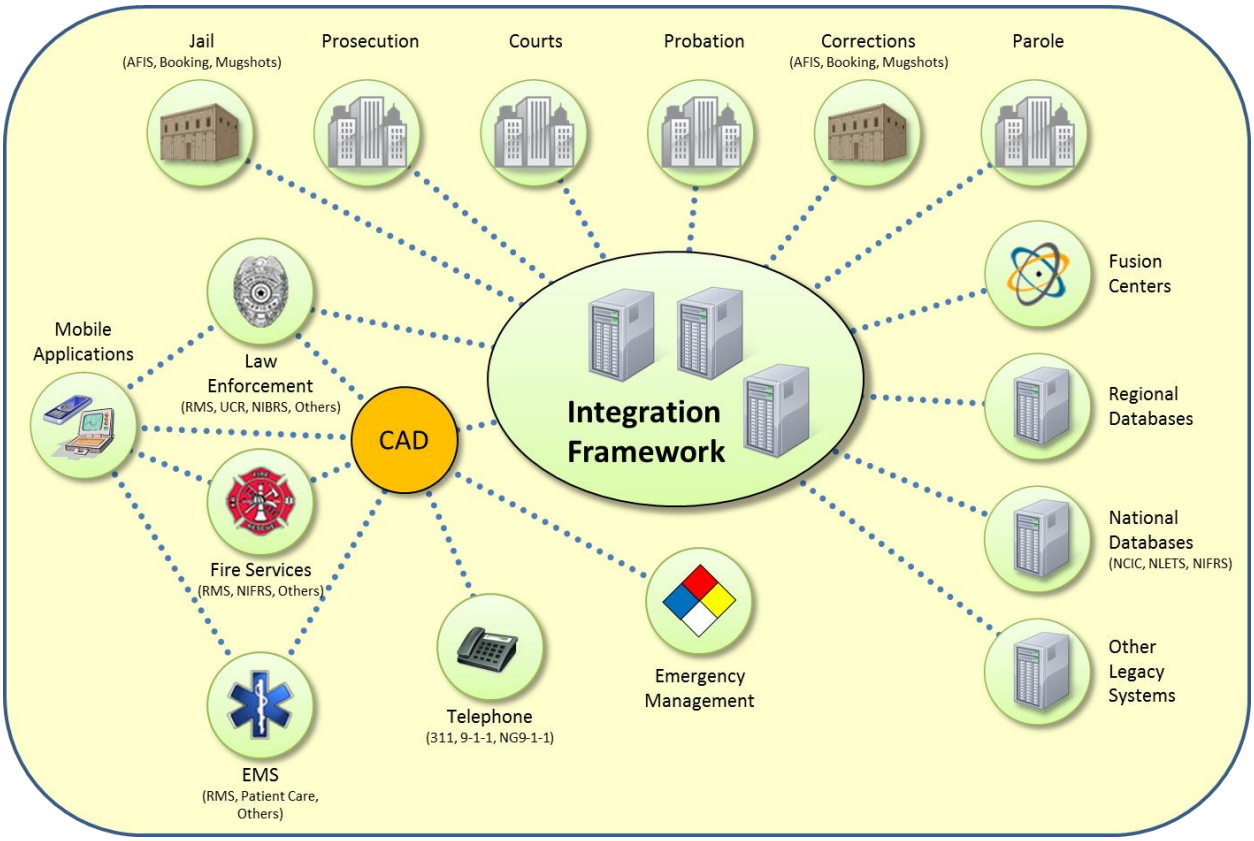
through their mobile data computers (MDC), remote connections, and/or other devices, such as personal digital assistants (PDA).

CAD systems are used to accomplish many tasks related to the tracking of public safety incidents and the assignment, allocation and deployment of law enforcement, fire, and EMS personnel. As well, CAD systems are designed and configured to meet the operational and administrative needs of the public safety agencies.

The CAD system is one of the most important tools utilized by a Public Safety Answering Point (PSAP). All reported incidents are entered, dispatched, managed, and tracked via the CAD system, making it a mission critical system. The lives of citizens and public safety personnel heavily depend on the CAD system consistently performing at its maximum operational effectiveness and reliability. Although a CAD system is just one of many systems that public safety departments utilize (see Figure 1 below), it is often considered the heart of public safety operations. Following are a few of many reasons for this:

1) Virtually all law enforcement, fire, and EMS incidents flow through the CAD system.
2) Many public safety technology systems, such as 9-1-1, Geographic Information System (GIS)/Mapping, Automatic Vehicle Location (AVL), MDCs, Records Management Systems (RMS), and data mining applications are either an integrated part of, or are interfaced with, the CAD system.
3) The CAD system is often the primary connection CAD users have to external systems, including neighboring and remote CAD systems, regional RMS, and state and federal criminal databases such as the Department of Motor Vehicles (DMV), Nlets (The International Justice & Public Safety Network), the Federal Bureau of Investigation National Crime Information Center (FBI NCIC), and the FBI's National Data Exchange (N-DEx).
4) The CAD system is the primary tool used for public safety resource management.

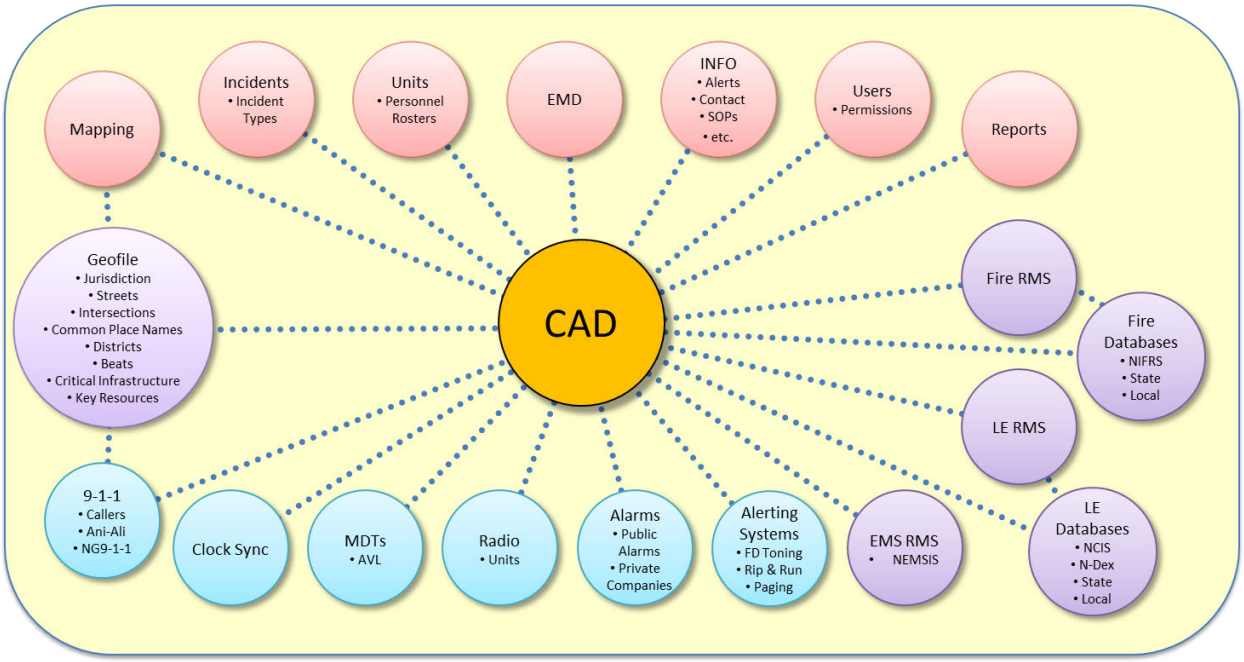
FIGURE 1. PUBLIC SAFETY SYSTEM INTEGRATION FRAMEWORK



CAD systems consist of several modules that provide a variety of services and functions at multiple levels within a public safety communications center (see Figure 2 below). These services include call input, call dispatching, call status maintenance, event notes, resource unit status and tracking, and call resolution and disposition.

Further, CAD systems include interfaces that permit the software to provide services to dispatchers, call-takers, and field personnel with respect to control and use of radio and telephony equipment, Emergency Medical Dispatch (EMD), external RMS, and other internal and external systems, as well as other services and functions.

FIGURE 2. CAD SYSTEM FUNCTIONAL COMPONENTS



1.2 Background

This section describes why the *UCADFR* document evolved and how it was developed.

2003-2006

The *Standard Functional Specifications for Law Enforcement Computer Aided Dispatch Systems* document was developed by the LEITSC to provide a starting point for law enforcement agencies to use when developing CAD RFPs; to level the playing field when working with software providers; and, to promote system interoperability (*e.g.* CAD-to-CAD). This document focused on CAD functionality to support law enforcement operations.

2009

The Public Safety Data Interoperability (PSDI) Project identified the need to expand the original LEITSC document to include CAD functions that support fire service and EMS dispatching, resulting in the release of the *Revision Assessment for the Incorporation of Fire and EMS Functions into the Law Enforcement CAD Functional Specifications*. This revision assessment provided the basis for determining the level of effort required to incorporate fire and EMS functional requirements into the existing *Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems* document, and specifically described fire and EMS CAD functionality that would need to be added. It also made numerous suggestions to modify the existing language and structure. Finally, it served as a supplement to the existing *Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems* to those needing a more complete list of base CAD functionality.

2010-2011

In response to the issues identified in the revision assessment document, APCO and the IJIS Institute, on behalf of the BJA, launched the Unified CAD (UCAD) Project in 2010. The UCAD Project was formed, in

part, to create this document, the *Unified CAD Functional Requirements* (*UCADFR*)—a detailed, comprehensive and unified set of functional requirements for CAD systems.

The project committee is comprised of 22 subject matter experts from various stakeholder disciplines (*i.e.* emergency communications, law enforcement, fire service, EMS, and industry). The *UCADFR* can be an invaluable resource to these communities by supporting the planning, acquisition and management of full-featured CAD software applications. The *UCADFR* identifies and describes over 130 CAD functions in 11 different topic areas and provides information on future issues for CAD systems, such as Next Generation 9-1-1 (NG9-1-1) and Broadband/LTE (Long-Term Evolution).

1.3 Notes to the Reader

Standardization of this Document

Since this document was made into a standard by APCO's American National Standards (ANS) process, it is critical to note that this standard/document does **NOT** standardize the functions that a particular CAD system **should** contain, but rather standardizes a "master list" of functions that a CAD system **COULD** contain.

Navigation

Rapid navigation to main functional areas or sub-functions is available from the Table of Contents and the Navigation pane. Each item listed includes a hyperlink that will navigate to the specific item when selected by the user.

Organization of Each Functional Section and Sub-Sections

Sections 2.0 through 11.0 in this document each correspond to a main CAD functional area with the associated functions for each. These include:

- **Call Handling / CAD Event Creation**

  Sub-Sections (Functions):

  - *Call Handling*
  - *CAD Incident / Event Types*
  - *Update Call for Service Event Data*
  - *Determine Dispatch Need*
  - *Utilize Incident Disposition*
  - *Assign Incident Classification and Priority*
  - *Check for Duplicate Incidents*
  - *Incident Information*
  - *Determining Capture Locations*
  - *Location Verification*
  - *Retrieve Incoming Calls*
  - *Involved Person Information*
  - *Involved Vehicle Information*
  - *Premises Hazards and Previous History*
  - *CAD Event Creation*
  - *Determining Response Agency and Service Area*
  - *Alarm Processing*
  - *CAD Event Routing*

- *Ability to Route to a "Decision Dispatcher"*

- **Dispatch Support**

  Sub-Sections (Functions):

  - *Run Cards / Response Plans*
  - *Adjustable Dispatch Levels*
  - *Additional Attributes*
  - *Mutual Aid Function*
  - *Automatic Aid Function*
  - *Unit Rotation (Unit Load Balancing)*
  - *Conditional Availability of Apparatus*
  - *Special Dispatch Areas*
  - *Emergency Medical Dispatch / Incident Triage*
  - *Channel Designations*
  - *Be On the Look-Out / Attempt to Locate*
  - *Dispatch Units*
  - *Resource Alerting*

- **Resource / Unit Management**

  Sub-Sections (Functions):

  - *Move Up ("Fill-In" and "Station Fill")*
  - *Staffed vs. Unstaffed Units*
  - *Cross-Staffing / Crew Counting / Shared Staffing Crew Accountability / Contingent Staffing*
  - *System Status Management (Dynamic Resource Deployment)*
  - *Additional Unit Status*
  - *Strike Team / Task Force Designations*
  - *Rostering*
  - *Scheduling*
  - *Mileage Tracking*
  - *Hydrant Location and Status*
  - *Additional Unit Dispositions*
  - *Exception Reason Tracking*
  - *Public Safety Flight Tracking*
  - *Geo-fencing*
  - *Station Dispatch*
  - *Pre-Release or Pre-Alerting*
  - *Vehicle / Unit Change*
  - *Automatic Driving Directions / Routing*
  - *Bypassed Units*
  - *Post-Dispatch Response Re-evaluation*

- **Call / Incident / Event Management**

  Sub-Sections (Functions):

  - *Display of Incident / Event Data*
  - *Update Incident Status*
  - *Dispatch Resource Decision*

- *Update Assigned Resources*
- *Update Supplemental Resources Tracking*
- *Assign Units*
- *Update Incident Data*
- *Assign Records Management System Incident / Case Number*
- *Transfer Basic Incident Data to the Records Management System*
- *Display Additional Incident Data*
- *Reopen Incident*
- *Add Destination Locations*
- *Hospital Status / Availability and Hospital Recommendation*
- *Patient Tracking*
- *Linking an Audio File to a CAD Event*
- *Multiple Simultaneous Incidents to Single Unit*
- *Scheduled Events*
- *Secondary Incident Location*
- *Single Discipline Incident to a Combined Discipline Incident*
- *Timers*
- *User Defined Status Timers*

- **Supplemental Resource Request and Tracking**

  Sub-Sections (Functions):

  - *Request Supplemental Resource*
  - *Request Supplemental Resource Rotation List*
  - *Notify Supplemental Resource Service*
  - *Enter and Update Supplemental Service Record*

- **Incident Disposition**

  Sub-Sections (Functions):

  - *Determine Incident / Event Status*
  - *Utilize Incident Management*
  - *Determine Report Functionality*
  - *Record Disposition*
  - *Send Data to Records Management System*
  - *Assign Agency-Specific Report Numbers*

- **Business Function: CAD System Administration**

  Sub-Sections (Functions):

  - *Geofile Maintenance*
  - *Security*
  - *Logging*
  - *Configuration*
  - *Table Maintenance*
  - *Communication Center / PSAP Relocation*
  - *CAD Catch-Up*

- **System Functions**

  Sub-Sections (Functions):

  - *Notifications*
  - *Contact List*
  - *Premises Information / Hazards*
  - *Communications Center / PSAP Standard Operating Procedures*
  - *Agency-Specific Incident / Location / Unit Standard Operating Procedures*
  - *Remote Access*
  - *CAD Workstation-to-CAD Workstation Messaging*
  - *Incident Command Support*
  - *Narrative Field "Shorthand" / Auto Text*
  - *Command Line / GUI*
  - *Date/Time Stamps*
  - *Unit Status Transitions Matrix*
  - *Single Sign-on for CAD and CAD Sub-systems*
  - *Multi-Agency / Multi-Jurisdictional Capability*

- **Reporting and Monitoring**

  Sub-Sections (Functions):

  - *Dispatch Supervisor Support*
  - *CAD Management Reporting*
  - *Training and Testing*
  - *Snapshot / Incident Replay*

- **Interfaces**

  Sub-Sections (Functions):

  - *Essential Interfaces*
  - *Additional Interfaces*
  - *Locational Systems Interfaces*
  - *Administration Interfaces*
  - *Communications Interfaces*
  - *Integration / Interfaces with Other Systems*
  - *National SAR Initiative Functionality*
  - *Emergency Operations Center Interface*

Each main functional area section provides:

- The name of the document section number and the main functional area (*e.g.* '3. Dispatch Support');
- A general description of the main functional area;
- Operational examples that apply to the main functional area; and,
- A list of possible functions within the main functional area that a CAD system could have.

Each possible function provides:

- The title of the document sub-section number and function (*e.g.* '3.1 Run Cards/ Response Plans');

- Icons below the function title to identify the service(s) that the function applies to (see the 'Icons' subsection below);
- A narrative that describes the function and when/how the function may apply;
- Sample requirements (see the 'Sample Requirements' subsection below); and,
- Relevant technical standards / guidelines, if known.

> Practitioners are reminded that this document is a living standard, maintained via APCO's ANS process. Readers should access the APCO Standards website[2] to obtain the most up-to-date information regarding a specific function, relevant standard, or guideline. For more information, please see Section 1.5.

Use of "Shall" and "Should"

The use of the word *shall* refers to a requirement, whereas the word *should* means that a specification is merely requested. It is the responsibility of each agency using this document to decide which specifications are mandatory and which are requested but not mandatory. Therefore, this document uses the phrase "*Shall* / *Should*" for each specification.

> Practitioners are expected to select the correct term for the desired system when adding the specification to the agency's RFP.

Icons

Icons are provided below the section title for each function included in the document. These icons are intended to provide a visual "flag" as to which service (Law Enforcement, Fire, EMS) the specification commonly applies to.

Law Enforcement 

Fire 

EMS 

Sample Requirements

The specifications presented in this document are representative and not intended to be all-inclusive.

> An agency planning to use this document to assist in the creation of an RFP or Request for Information (RFI) should edit any sample requirements used for that purpose to conform to the particular agencies' particular needs and requirements.

[2] For more information, please visit the 'APCO Standards for Download' webpage: http://www.apco911.org/resources/9-1-1-resources/standards/apco-standards-for-download.html

It should be noted that many of the sample requirements may not be appropriate for smaller communications centers. Thus, care must be taken when constructing an RFP based on the requirements included in the *UCADFR* to avoid needlessly increasing the cost and complexity of the procured CAD system. Functions may have a single sample requirement, while others may have multiple sample requirements based on the complexity and/or scope of the function.

> For agencies creating an RFP for a CAD system, do not limit yourself to the functions in this document. You may have a need that is not included.

Generic / Provider Agnostic

The information presented in this document is intended to be generic rather than favoring one particular system or approach over another. The document defines *what* is to be accomplished versus *how* it should be accomplished. These requirements were developed to depict current, basic functionality that a new CAD system might contain.

Incidents/Events/CFS

For the purposes of this document, an *incident* is a real world event that results in a notification being made to a PSAP. An incident could range from something as minor as a parking complaint, as routine as an officer initiating a traffic stop, or as major as a natural disaster or terrorist attack. Once the PSAP has been notified, the CAD operator creates a CFS, CFS event, or CAD event in the CAD system for the purpose of tracking the incident. The CFS or CAD event is the CAD record of an incident occurring in the field. A single incident can result in multiple CFS and/or events. All pertinent information relating to the actions taken by one or more communications centers is accomplished through one or more CFS event records. Generally, a CAD CFS event record is created when an incident requires the dispatch of one of more resources, including officer-initiated activities.

Questions/Suggestions

For questions about the functions in this document, please contact the National Information Sharing Standards (NISS) Knowledge Base and Help Desk:

- *Web*: http://it.ojp.gov/framesets/niss-noClose.htm
- *Email*: NISShelp@ijis.org
- *Phone*: 877-333-5111 or 703-726-1919

1.4 Using This Document for RFP Creation

This section deals with the functional requirements section of the RFP only.

The Project Committee recommends the following for persons who plan to use this document to assist in the creation of an RFP for a CAD system:

- Do **NOT** include in your RFP a requirement to "conform to the requirements of the *UCADFR* document" or similar language. This document is generic, as evidenced by the inclusion of both '*shall*' and '*should*' for each requirement, and thus will not give you the specific information you may need to evaluate CAD systems. CAD providers cannot appropriately respond to a RFP where all requirements are deemed both mandatory and "nice to have."
- If you have a base RFP created, then review this document for additional functionality and/or requirements you want to add. Remember that you will need to decide whether each

requirement will be a '*shall*' (mandatory) or '*should*' (desired) item depending on your agency's needs/desires.

When starting to write an RFP from scratch:

- Review this document for functionality you need or desire.
- Determine which functions are required for your operations and which are "nice to have."
- Select the requirements for each of the functions you selected, and write additional ones to fully describe what you are looking for. Make sure to include any specifics you can – the more detailed and clear the requirement, the better and more accurate the responses you will get. Make sure to include a "lead-in" (*e.g.* "In order to support the Call Handling Function, the CAD system…"), so that the requirements can be understood.
- Edit all requirements with regards to '*shall*' (mandatory) or '*should*' (desired). Be realistic in your determinations.

For more information, see the *IJIS Institute's Pre-RFP Toolkit* at:
http://www.ijis.org/_resources/pre_rfpCD.html.

1.5 UCADFR as a Standard

Updates to the Standard

As a living standard, this document is subject to periodic update via the APCO ANS. Any stakeholder may submit suggested additions, modifications, or deletions to APCO for consideration in the next version. Decisions on modifications are made by a committee of subject matter experts. Potential modifications include but are not limited to:

- Functions
- Descriptions
- Sample Requirements
- Technical References / Guidelines

To submit suggestions, email standards@apcointl.org.

Pending Modifications

It is important to stay informed of the latest approved/pending modifications to this standard. To do so, go to http://www.apco911.org/911-resources/unified-cad-project-ucads.html.

2 CALL HANDLING / CAD EVENT CREATION

The CAD handling and event creation process consists of the PSAP being notified through a variety of sources of the need for assistance:

- Receiving a telephone call, electronic notification, radio request;
- Obtaining sufficient and accurate information from a reporting party or electronic device to determine the location and event classification;
- Determining if the incident being reported is a duplicate of an incident in progress; and,
- Creating or updating the CFS in the CAD system.

The system should provide users an automated process to verify, analyze, classify, and prioritize CFS before electronically routing them to dispatcher(s) or to other appropriate destinations, such as a telephone reporting unit. CFS may also be generated by units in the field via their MDC or generated by a monitoring device such as an accident detection unit, intrusion alarm, or personal health monitor and transmitted to the appropriate communications center via a data interface.

Operational Examples

A traffic accident occurs at a busy intersection and it is obvious to witnesses that injuries are severe. Smoke is emanating from one of the involved vehicles. Information is gathered from the first 9-1-1 caller and entered into the CAD system using a CAD event data entry screen. The call taker enters the event's location into the CAD system and selects the appropriate event type based on information provided by the reporting party. The call taker enters the event so the CFS can be simultaneously sent to the appropriate law enforcement, fire, and EMS dispatch positions. Dispatcher positions are now able to immediately assign and dispatch emergency resources to the event by using pre-determined response plans, which are based on the event's location and type.

Meanwhile, the call taker continues to gather additional information from the reporting party and updates the CFS record. Each involved dispatcher receives notification that the CFS has been updated and is able to view the updates. Other people may dial 9-1-1 or a non-emergency number to report the same incident, or an accident detection device on one or more of the involved vehicles may also report the accident. As call takers begin the data entry process, the CAD system alerts them that a CFS is currently active for the same location and has a similar event type. The call taker can then determine whether the new reporting parties have additional information that was not reported by the initial reporting party. A new CAD event entered but later determined to be a duplicate of a CAD event already in progress can be flagged in the CFS record as a duplicate of the original incident. Pertinent details gained from these new reporting parties can be provided as updates to all involved dispatchers and field responders.

2.1 Call Handling



A reporting party initiates the CAD process by reporting an incident to a public safety answering point. *Reporting parties* consist of citizens, electronic devices (*e.g.* burglar or fire alarm), agency staff, and other agencies requesting services from the agency or giving notification of events or activities of concern. An incident notification may come from many different points of origin, such as alarm systems, personal monitoring devices, Enhanced 9-1-1 (E9-1-1) systems, direct calls (10-digit numbers), walk-ins, CAD-to-CAD interfaces, two-way radios, and other Web-based systems.

The service requested by reporting parties can consist of both emergency and non-emergency priorities. *Call taking (handling)* consists of:

- Receiving the call or other notification;
- Obtaining sufficient information from the reporting party;
- Determining if the event reported is a duplicate of an incident in-progress; and,
- Recording or updating the CFS in the CAD system.

The call taker may also apply procedures and guidelines to verify, analyze, classify, and prioritize the CFS prior to routing it to appropriate dispatch positions. A CFS may also be generated by a unit in the field when a field unit encounters a new incident or when the field unit self-initiates an activity. The unit can contact the dispatcher or the call taker, or may electronically create the CFS using their MDC or other device with a CAD-accessible application.

A CFS may be forwarded to a telephone reporting unit or be initiated by the telephone reporting unit. A telephone reporting unit typically handles non-emergency CFS in response to incidents that do not require a response by field resources.

A CFS may be created for future scheduled events, such as parades, organized demonstrations, and large concerts.

Sample Requirements

In order to support the *Call Handling* function, the CAD system:

- *[Shall/Should]* import and attach/append, automatically upon user command, automatic number information (ANI) and automatic location information (ALI) to a CFS.
- *[Shall/Should]* import (automatically) external alarm data that conforms to the APCO/CSAA (Central Station Alarm Association) published ANS; and, *[Shall/Should]* generate a CFS upon receipt of a new alarm notification.
- *[Shall/Should]* import (automatically) a CFS received from another CAD system.
- *[Shall/Should]* import (automatically) a CFS generated on an MDC.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.2 CAD Incident / Event Types



CAD incident/event types describe the nature of "what is happening" at an incident. They are codes that describe the various types of incidents that can be received by a PSAP. Typically, each incident type is associated with a specific response plan that establishes the number and types of resources initially required for mitigating the incident, dispatch position(s) responsible for the incident, and its default priority.

CAD systems should allow specific instructions to be associated with CAD event types that may, for example, display specific questions regarding the nature of the incident (type) thereby assisting in a better classification of the incident. If present, CAD should display the special instructions after the event type is entered. The special instructions can be presented to the CAD user as text, drill down

trees, or other similar methods. If a tree format is used, then the selected responses should be stored in the event history.

Special CAD Incident Types

A *CAD incident type* (nature code/event type) can initiate multiple CFS events if the incident type is determined to require a multi-agency response (*e.g.* an accident with injuries in which law enforcement, fire, and EMS must respond). Available options for dealing with this situation may include creating a separate, but linked, CFS event record for each required service agency, or creating one CFS event record that handles all of the responses. The selected method should be compatible with the local agency's requirements.

Although APCO, National Emergency Number Association (NENA), and other national and international public safety organizations are moving towards a national set of defined incident types, CAD systems should allow the local agencies using them to define and update their own sets of incident types. CAD systems should also allow agencies to associate incident types with specific dispatch plans and priorities. CAD systems should allow the local agencies that create their own sets of incident types to map them to the appropriate ANS incident types so that incidents can be more easily shared across agencies and CAD systems. Some examples of typical user-definable specialized incident types include hazardous materials, weapons of mass destruction (WMD), decontamination, bomb threat, and civil disturbance.

Advised Events

CAD systems should provide users the ability to record information from citizens about particular situations or events that do not require the dispatching of any public safety resources. These incidents should create CAD event records that are recorded and that can be easily retrieved from the system/event history files for later access and analysis.

CAD systems should also be able to route advised events to pre-defined workstations, user groups, and/or a pre-determined set of locations, such as fire stations, based on the dispatch plan associated with the incident's event type and location.

CAD systems should support the capability of pre-determining that a specific event type will automatically become an advised event with specific notification/routing characteristics. In addition, a CAD user should be able to designate an event as an advised event during event entry.

Advised events should be able to initiate agency-definable notifications.

Make Paper Events[3]

CAD system users should be able to enter an event that bypasses dispatch, but that assigns a resource with a disposition and closes the event upon entry with the user designated disposition. This "Make Paper" event should be included in the location history of the location where the event occurred. It should be possible to associate "Make Paper" events with a logged-on employee's identification. A "Make Paper" event identifier in the event history should differentiate it from normal events.

Sample Requirements

In order to support the *CAD Incident / Event Types* function, the CAD system:

- *[Shall/Should]* allow for system administrator-defined CAD incident types or nature codes.
- *[Shall/Should]* allow system users to modify the incident type and provide new/updated response plan information/suggestions based on the new incident type.

[3] Also known as a "Log Only Event" by some agencies.

- *[Shall/Should]* provide the capability to create an event, assign a unit, and close the event with a disposition without going through the dispatch process steps.
- *[Shall/Should]* provide the capability to flag a CFS as an "Advised Event" separate from the incident type/nature code.

Relevant Technical Standards / Guidelines

- *APCO 2.103.1-201x: Public Safety Communications Common Incident Types for Data Exchange* (in development) – http://www.apco911.org/911-resources/standards/apco-standards-in-progress.html.

2.3 Update Call for Service Event Data



As new information about an incident is obtained from the reporting party or other reporting sources (*e.g.* field responders reaching the scene, monitoring devices, duplicate calls), CAD systems must provide a mechanism for entering the new information into the CFS record. New information that surfaces about an open incident must update the CFS as new information becomes available. Multiple callers provide potential witnesses to the incident and may provide additional or supportive information. This may result in the reclassification and/or re-prioritization of the incident. Communications center personnel must be able to enter narrative data and the reporting parties' information into the CFS record at any time before and after the event is closed.

Sample Requirements

In order to support the *Update Call for Service Event Data* function, the CAD system:

- *[Shall/Should]* enable the user to enter supplemental (new) information into the CFS event record of one or more user-specified CAD events.
- *[Shall/Should]* display a notification of the event update at each appropriate CAD position whenever an active event record is updated, as determined by the system's configuration.
- *[Shall/Should]* create an automatic time/date stamp for every transaction related to an event, and *[shall/should]* store the responsible operator's identification (ID), the console ID, and the nature of the change.
- *[Shall/Should]* add audit records to the event history or store audit records in the CAD system's audit log file in chronological order; and, *[Shall/Should]* provide a complete historical audit of all event activity (*e.g.*, comments, unit status changes, license plate information, field updates).
- *[Shall/Should]* store old entry information, with the appropriate date, time, operator ID, and console stamps if the new entry replaces existing information in the event record.
- *[Shall/Should]* enable the audit information to be retrieved and printed in both summary and detailed formats when incident information is displayed.
- *[Shall/Should]* create a permanent audit trail for all information recorded related to an event, whether or not that information is later modified or deleted.
- *[Shall/Should]* support ease of entry for supplemental event information and changes to existing event information.

- *[Shall/Should]* allow the user to display a supplemental data entry screen by specifying either the event number or a unit assigned to the event.
- *[Shall/Should]* allow the user to display a data entry screen to change information previously entered into a CAD event by specifying either the event number or a unit assigned to the event.
- *[Shall/Should]* provide agency-definable visual and audible alerts to notify field units and other appropriate CAD system users, including users of systems interfaced to CAD such as Mobile Data Computers, of event changes and supplemental information.
- *[Shall/Should]* allow the user to add supplemental information and/or change active events.
- *[Shall/Should]* allow the user to update any field in the CFS event record (except user-designated fields, such as application-generated times and date stamps, operator identification information, ANI/ALI information, and CAD position that completed a CAD transaction).
- *[Shall/Should]* document all changes and supplemental information in the event history.
- *[Shall/Should]* provide an event update/change data entry screen.
- *[Shall/Should]* allow the user to update or change a unit's most recent event by entering the unit's identification or any unit that is currently assigned.
- *[Shall/Should]* require confirmation from the user when attempting to update any field in a closed event.
- *[Shall/Should]* provide the user with acknowledgment that an update to a CAD event record was successfully completed.
- *[Shall/Should]* allow the user to supplement and/or change active events.
- *[Shall/Should]* allow the user to supplement and/or change any field of a closed event without having to change the state of the event.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.4 Determine Dispatch Need



For every CFS, a decision must be made as to whether to dispatch resources or to close the CFS with an explanation of why no resources were dispatched.

If the information gathered indicates that a public safety response is not warranted, based on local policies and protocols, then the CFS should be closed with a disposition code and, where appropriate, narrative/comment information that explains why no resources were assigned to the event.

If a decision is made that resources are required, then the collected information must be routed to a dispatch position to begin the resource assignment process. As noted throughout this document, these two functions (call taking and dispatch) can be performed by the same person.

Sample Requirements

In order to support the *Determine Dispatch Need* function, the CAD system:

- *[Shall/Should]* provide the capability to close out the CFS record without assigning a resource, if it is determined that a CFS does not require the assignment of a resource(s).
- *[Shall/Should]* allow the user to append a disposition code and comments to events that are not assigned any resources.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.5 Utilize Incident Disposition



An incident is normally considered closed when all assigned units have completed their assignment and have cleared from the incident. Depending on the agency's standard operating procedure (SOP), the primary unit, a dispatcher, or both must be able to close the CFS and append a disposition code/status to the incident's record. Dispatchers are typically notified of changes in status and locations of the resources that they are controlling, either via radio (voice) or MDC transactions. Unit status and location status changes completed via MDC transactions should automatically update the CAD system. The CAD system should automatically close an event if the received MDC data indicates that the incident is complete by determining that resources are no longer assigned to the incident. Prior to closing the call, a specific closing disposition must be added to the CFS record if required by agency policy. Typically, the incident's final (closing) disposition is provided and/or entered by the incident's primary unit. Depending on agency SOPs, other assigned resources may also be required to provide one or more dispositions when clearing from their assignments.

When a CAD event is closed, and at other times during the incident, CAD must be able to automatically transfer key event information to one or more associated RMS. Any updates made by CAD users on reopened incidents should also be automatically transferred to the appropriate RMS, subject to agency policies (see Section 11.1 Essential Interfaces).

When a duplicate event is identified, CAD users must be able to close the duplicate event with a disposition indicating that it is a duplicate event. CAD users must be able to merge any new information contained in the duplicate event into its equivalent main CAD event. The CAD system must automatically cross-reference the main and duplicate events before closing them so that either one can be retrieved, if necessary.

Sample Requirements

In order to support the *Utilize Incident Disposition* function, the CAD system:

- *[Shall/Should]* allow the user to enter one or more dispositions, as dictated by agency policy, when a CAD event is closed.
- *[Shall/Should]* close a CAD event record automatically if no resources remain assigned to the event.
- *[Shall/Should]* provide the capability for a mobile unit to enter one or more dispositions when clearing from a CAD event.
- *[Shall/Should]* allow the system administrator to define disposition codes.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.6 Assign Incident Classification and Priority



One of the key pieces of information utilized in CFS event creation is *incident/event classification*. This process will determine the appropriate dispatch and response needs.

A list of pre-defined incident type codes created by the system administrator is presented to CAD users to allow the most appropriate incident type to be selected. Each of these codes has a default priority assigned based on agency, geo-area, response plans, and deployment plans. The priority and response criteria can be specified for each agency, based upon individual policy. Upon completion of this task, a type code is assigned to the incident.

Based upon information gathered, the incident classification process should be able to be upgraded or downgraded as the incident details depict.

When using a system that serves multiple jurisdictions, this step should be able to create a CFS event for each response agency with one entry.

Sample Requirements

In order to support the *Assign Incident Classification and Priority* function, the CAD system:

- *[Shall/Should]* enable CAD users to select the appropriate incident/event type from a pre-defined list of codes based upon information received from reporting party.
- *[Shall/Should]* provide, in a multiple dispatch agency or jurisdiction environment, the ability to create multiple CFS events with a single CFS event entry (*e.g.* a shooting incident type would create a law enforcement, EMS, and possibly a fire event).
- *[Shall/Should]* provide the ability to generate a CFS event with only the location and incident type code entered.
- *[Shall/Should]* allow the user to upgrade or downgrade the CFS event to fit the reported event by changing the priority for the event.
- *[Shall/Should]* allow the user to utilize incident screening menus, such as a drop-down menu, to assist in determining the appropriate incident/event type code.
- *[Shall/Should]* allow the user to interrupt the CFS event creation process and save entered information, sometimes known as call stacking, to process a higher priority incoming incident.
- *[Shall/Should]* provide a warning notification of the held CFS event generated at an administrator-configured time. Any position can review current CFS events, retrieve a partial CFS record, and complete the CFS event entry.
- The number of partial CFS events that can be stacked by a single position *[Shall/Should]* be an administrator-configurable system parameter.
- *[Shall/Should]* provide the ability to override the event priority for each agency.
- *[Shall/Should]* provide the ability to create and maintain incident screening menus or prompts that can be used to aid the call taker in determining the appropriate incident/event type code.

- *[Shall/Should]* provide the ability to save one or more partially completed CFS events in order to enter a higher priority incident, keeping all entered data intact.
- *[Shall/Should]* provide a warning (visual and/or audible) that a partially completed CFS event has been held for an administrator-defined period of time.
- *[Shall/Should]* provide the ability to view a summary of all system-wide, partially-completed CFS events being held and awaiting completion.
- The summary *[Shall/Should]* include, at a minimum, the position and user ID that placed the CFS event on hold and the elapsed time that the CFS event has been on hold.
- *[Shall/Should]* provide the ability to redirect assigned resources to a higher priority CFS event based on agency defined criteria.
- *[Shall/Should]* store all active and partially completed CAD events in system administrator-configurable queues.
- *[Shall/Should]* allow CAD users to be able to select a partially completed CFS event from a CAD event queue and complete the CFS entry process.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.7 Check for Duplicate Incidents



Multiple incident notifications for the same incident may be received via many sources; for example:

- A traffic accident is witnessed by two or more motorists, an on-duty public safety responder, and by a Telematics[4] Service Provider (TSP); or,
- A fire alarm is reported from an electronic monitoring system and, at the same time, a witness calls 9-1-1 reporting smoke coming from a business.

CAD systems must be able to automatically evaluate an entered incident's location and call type to determine whether it is a duplicate or new CAD event. The duplicate event detection process must be based on pre-determined geographic search parameters that include exact street addresses, street addresses within the same block, system administrator-configurable radius searches around the geo-coordinates of the incident location, and/or other system administrator-defined search parameters. The CAD system should analyze all open events, as well as closed events, within an administrator-configurable time period. Upon indication by the CAD system of a possible duplicate event, CAD system users must be able to evaluate the duplicate event detection information presented by the system to make the final decision of whether new incident notifications are duplicates of a previously entered CAD event.

[4] *Telematics* is the blending of computers and wireless telecommunications technologies, ostensibly with the goal of efficiently conveying information over vast networks to improve a host of business functions or government-related public services. The term has evolved to refer to automobile systems that combine global positioning satellite (GPS) tracking and other wireless communications for automatic roadside assistance and remote diagnostics. The telematics industry is not limited to automotive applications. Other applications are being studied or developed for monitoring water and air pollution, for medical informatics and health care, and for distance learning.

If the new incident is determined to be a duplicate, then CAD users should be able to add any new information contained in the current CFS entry screen and link the new information to the primary active CFS record without having to re-enter it. Based on agency policies, events linked to the primary active CAD event record should be automatically updated by the CAD system to contain the newly added information, and CAD users should be alerted that new information is available in the linked call's event record.

If the primary event record associated with a duplicate CAD event is closed, then CAD users should be able to add new information to the closed event record, possibly with a reminder to the user that the record was closed. If the new information requires a dispatch of public safety resources, then CAD users must be able to re-open the CFS event, add the new information, and route the CFS back through the dispatch process.

Sample Requirements

In order to support the *Check for Duplicate Incidents* function, the CAD system:

- *[Shall/Should]* store all transactions resulting from the duplicate event detection process in the system's audit log.
- *[Shall/Should]* identify during the creation of a CFS event whether the event is a potential duplicate of an active CAD event or an event recently closed; and, *[Shall/Should]* notify the call taker of the results.
- *[Shall/Should]* check, as configured by the system administrator, by exact street address, street address block range, or geo-coordinates, the location of each new CFS event to determine whether another event exists.
- Based on system parameters set by the administrator, either all matching events *[Shall/Should]* be presented to the user, or only those events with the same or similar nature code.
- *[Shall/Should]* check, as configured by the system administrator, within a pre-defined search radius of the location of each new CFS event, to determine whether another event exists within the search radius.
- Based on system parameters set by the administrator, either all matching events *[Shall/Should]* be presented to the user, or only those events with the same or similar nature code.
- *[Shall/Should]* allow an authorized user to change the duplicate event search parameters (*e.g.* distance, exact street address match only, street address block range).
- *[Shall/Should]* present the user with the following information for each potential duplicate event if potential duplicates are located:
    - Incident ID
    - Type of incident
    - Location of the incident
    - Status of the incident
- *[Shall/Should]* allow the user the ability to create a new CFS event and link the event to the primary event record; or, to merge any new information contained in a duplicate event into the main event record associated with the identified duplicate CAD event.

- *[Shall/Should]* allow the call taker to re-open closed CAD events that are duplicates of a new event, add additional information to the re-opened CAD event records, and, if necessary, re-route them back through the dispatch process.
- *[Shall/Should]*, based on agency policy, restrict users from changing or deleting any previously entered data contained in re-opened closed CAD events.
- *[Shall/Should]* cross-reference duplicate events to the primary event records, leave both events open, or abandon processing of the duplicate event.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.8 Incident Information



There are several means for receiving requests for assistance from the public: telephone, from a field unit via radio or MDC, through a CAD-to-CAD interface, via telematics monitoring devices, and directly from third-party alarm-monitoring centers. Most, if not all, of the information received from the public or from an interfaced device (*e.g.* CAD-to-CAD, alarm monitoring) needs to be captured in the event's CAD record. This section deals with incident information that needs to be captured by CAD.

Call takers acquire *incident information* (*e.g.* the reporting party's name/address/phone number, incident location, narrative details, incident location, affected business name, incident location directions) from reporting parties and automated devices. Depending on how the reporting party contacts the PSAP, some of this information, such as ANI/ALI, is available through digital displays and interfaces.

Either before being entered into CAD or immediately after (if automatically loaded into CAD via an electronic interface), all of this information must be verified and validated. CAD systems must provide an ergonomically structured, easy flowing graphical user interface (GUI) that can be used to enter and/or validate incident-related information.

Although call takers need to be able to enter information into CAD in any order, the location, nature of the incident, and caller phone number are prioritized: call takers typically interact with reporting parties in a structured manner that enables obtaining these three critical components of the incident as quickly as possible. Once these critical components are obtained and verified, and depending upon the priority of the incident, CAD must be able to route this partially completed event record to appropriate dispatchers so that resources can be assigned and dispatched while call takers continue collecting other incident information from reporting parties.

CAD users (*e.g.* telecommunicators, dispatchers, call takers, supervisors, and even first responders) must be able to enter narrative information (comments) into the CAD event record. Since more than one CAD user and first responder could be working on a single CAD event, and since dispatchers and first responders need to be aware of all recently entered/updated information, CAD must support the continuous and simultaneous entry of comment information into the CAD event record by multiple users. As comments are entered into CAD, they must be almost instantaneously available to all staff handling the event.

Structured, drop-down, data entry fields should be available for those emergency event-related data that lend themselves to standardization (*e.g.* height, weight, priority, nature code/type, incident location). Free format fields (*e.g.* text comments and descriptive fields) should also be available as needed. CAD system users should be able to enter text in a non-case sensitive format, as well as to use search, replace, spellcheck, and other text editing features when appropriate. CAD systems should provide the ability to enter an unlimited number of comments/narrative details.

As NG9-1-1 capabilities become more widespread, CAD systems should be compatible with handling NG9-1-1's enhanced media content (*e.g.* pictures, text, streaming audio and video, and telematics data streams), including the display, storage and retrieval of this information from the CAD system and/or an interfaced recording device/system. Sample Requirements

Sample Requirements

In order to support the *Incident Information* function, the CAD system:

- *[Shall/Should]* provide the ability to create a CFS with minimum required fields (*e.g.* location and event type).
- *[Shall/Should]* provide the ability to dispatch once location and nature are obtained.
- *[Shall/Should]* provide the ability to alter/augment event as further information is obtained by the call taker.
- *[Shall/Should]* include an automated connection/interface to the 9-1-1 telephone system to use ANI/ALI data to populate the incident entry screen form.
- *[Shall/Should]* provide the ability to use ANI/ALI data to assist with CFS entry.
- *[Shall/Should]* provide the ability to enter unlimited narrative with text wrap-around feature.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.9 Determining Capture Locations



In many instances, call takers have access to callback numbers and call origination locations (ANI/ALI) via the E9-1-1 system. If not, then the incident location must be elicited from the caller. In some incidents, the caller's location is not the location of the incident (*e.g.* fire across the street, accident report from a moving vehicle).

Different ANI and ALI information is provided, depending on whether the emergency call is received via a landline/Voice over Internet Protocol (VoIP), E9-1-1 call, a wireless phase I (WPH1) mobile 9-1-1 call, or a wireless phase II (WPHII) mobile 9-1-1 call:

Landline/VoIP 9-1-1 trunk

- Physical address, the name of the account holder, call back phone number and response agencies for law enforcement, fire, and EMS at that location through use of an Emergency Service Number (ESN)

Some ALI addresses may contain a community name that is based on the telephone exchange office or central office location, and not a postal/civic compliant city name.

Wireless 9-1-1 trunk

- *WPH1*—Cellular tower address and latitude/longitude, call back phone number, and Telco ID
- *WPH2*—Cellular tower address, latitude/longitude and possibly altitude of caller, callback phone number, and Telco ID

Class of service designations may vary between local exchange carriers (LECs) and competitive local exchange carriers (CLECs)—for example, for WPH1 service, one carrier may provide a class of service labeled "WPH1," whereas another carrier may label the class of service "WRLS."

If on a business line and the agency has Caller ID (*i.e.* shows the telephone number of the caller), then the telephone system will display the call back phone number and account holder's name.

Under NG9-1-1, a wealth of additional data will be available to the call taker, including the call back number, a validated civic address, an X,Y coordinate representing the caller's location, a Z coordinate to represent the caller's altitude or elevation, and additional premises (*e.g.* key gate codes, after hours contact information), as well as individual information (*e.g.* medical condition, medical history) that may have been collected and stored in the event that a 9-1-1 call was made by the individual at that specific location.

CAD systems must provide an automated means for loading all location and location-related information available from the system on which the emergency (9-1-1) call was made into the CAD event record without requiring the information to be manually re-entered. CAD should provide an easily enabled procedure GUI interface for verifying the information provided by the phone system.

Sample Requirements

In order to support the *Determining Capture Locations* function, the CAD system:

- *[Shall/Should]* obtain all different versions (Standard, Standard Plus, Extended Plus) of ANI/ALI information automatically from interfaced phone systems without requiring the user to manually re-enter the information into a CAD event entry screen.
- *[Shall/Should]* append 9-1-1 reported data to the record if the user has entered data into any field before accepting the 9-1-1 information, but not overwrite the data entered by the user.

Relevant Technical Standards / Guidelines

- *NENA 02-10 v9 – Data Formats for ALI, MSAG & GIS* – http://www.nena.org/?page=Standards
- *NENA 02-11 v7 – 9-1-1 Data Management* – http://www.nena.org/?page=Standards

2.10 Location Verification



CAD event locations should always be validated (*i.e.* checked) against a geographic file (geofile[5]) that includes all of the current addresses for the area under the control of the communication center. CAD systems should contain an easily-invoked tool to assist users in validating entered locations. The tools may vary in how they operate, but should include prompts and ordered lists that present the user with suggested addresses/locations when the exact address cannot be validated.

Locations that cannot be verified provide an indication that the location information may be inaccurate. In these situations, the call taker may need to collect additional information that may be stored in a narrative format (*i.e.* as comments) in the CAD event record to assist dispatchers in assigning the proper resources, as well as guiding emergency responders to the correct location of the incident.

When a call is misrouted due to an inaccurate location, a complicated boundary scenario, or some other reason, and results in the wrong jurisdiction being notified, the call taker should either transfer the caller to, or notify, the proper jurisdiction, depending on agency SOP.

Incident locations vary in format and at least the following location formats should be supported by CAD systems:

TABLE 2. LOCATION FORMATS

INCIDENT LOCATION	EXAMPLE FORMAT
Civic address	123 Main Street, Anytown USA 98765
100 block face	The 300 block of Main Street
Intersection	1st Avenue and Main Street, Anytown USA 98765
Geo-coordinates	Latitude and longitude, decimal degrees referenced to the North American Datum of 1983 (NAD83), X,Y
Common place name/landmark	Joe's Bar and Grill in Anytown USA, Anytown City Hall, McArthur Park in LA
Mile markers	Mile marker 26 on HWY 45 North
Free format description	Behind the red barn on rural road 26 about 5 miles past Joe's farm

Location information for common places and landmarks should include a street address cross-reference or appropriate geo-coordinates that provide the legal street address/location for that common place/landmark.

Location validation information and other geographic data are typically contained in the CAD system's geofile. Geofiles typically contain street centerline information, along with appropriate latitude, longitude and, optionally, altitude information for each street center line segment, as well as attributes describing the addresses contained on each side of a street centerline segment. In addition, CAD systems should support structure file-based geofiles that contain street center line data, plus all of the unique structures within a portion of (*e.g.* the urban portion) or the entire CAD system's service area. As NG9-1-1 call routing and media support are implemented, CAD systems will have to support increasing

[5] A *geofile* is a set of spatial data sets organized either in a graphic or tabular format that represent the street network, specific locations, and relevant geographic boundaries within the geographic area in which a CAD system is deployed. The street network stored in the geofile is often used to locate incidents and responders and (as a topological network) to aid responders to navigate to the location of an emergency event. Geographic boundaries available in a geofile are often used to determine which agency is responsible for an emergency incident and the specific responders that should handle the incident. The street network, specific locations, and the geographic boundaries available in a CAD geofile are often used to support analysis and management decisions.

levels of detail—for example, in the future under NG9-1-1, parcel and structure boundaries may need to be supported by CAD geofiles.

The CAD system's geofile should assist users to:

- Validate the street name is an actual street in the service area
- Resolve ambiguities, while accounting for spelling variations and duplications
- Validate intersections
- Validate address ranges
- Relate common place names to actual addresses
- Relate latitude, longitude, altitude (X,Y/Z) coordinates to an actual address
- Transform latitude and longitude to map coordinates for display
- Translate incident locations to agency reporting areas
- Translate alias names to actual street names
- Display high and low cross streets
- Display city and county, neighborhoods/localities
- Assign and display the law enforcement, fire, and EMS response areas containing an incident
- Assign and display the law enforcement, fire, and EMS map pages where an incident is located
- Display CAD system premises warnings or hazards based on the location of incident(s)
- Display CAD system premises warnings or hazards based on the incident type that are within a configurable radius of incident locations
- Display prior incidents that occurred at an incident's location within a configurable period of time
- Display nearby fire hydrants
- Display nearby incidents (user-defined criteria)

Sample Requirements

In order to support the *Location Verification* function, the CAD system:

- *[Shall/Should]* provide the ability to enter a unique building and unit number to clearly identify the location (*e.g.* 100 West Ave., Bldg. 2, Unit 1).
- *[Shall/Should]*, depending on the permissions granted to the user, provide the ability to edit ALI 9-1-1 information in the event record if the information provided by the phone company is incorrect.
- *[Shall/Should]* include the following fields for all records containing an address: street number; apartment/suite number; street; road type (Drive, Avenue, Street, Alley); direction; city, state, and/or zip code (modify list as appropriate).
- *[Shall/Should]* validate entered incident addresses against the CAD geofile.
- *[Shall/Should]* provide various suggestions to assist users in selecting accurate incident locations.
- *[Shall/Should]* allow each address or commonplace name to have an unlimited number of alias names.
- *[Shall/Should]* allow authorized users to store multiple names for businesses and tenants for a given street address.

- *[Shall/Should]* organize the display of possible address matches in an ergonomic, easily understood manner that aids users in identifying valid incident locations.
- *[Shall/Should]* allow authorized users to configure their tactical map display to show jurisdictional boundaries (*e.g.* city boundaries) and to display potential valid incident locations by jurisdiction.
- *[Shall/Should]* allow the user, in case the location entered by the user is unverifiable (*e.g.* the location does not exist in the geofile), the capability to exit or bypass the verification process and manually route the CFS event(s) to the appropriate dispatch position(s).
- *[Shall/Should]* provide the ability to enter a partial street name, with a minimum number of characters, and be presented with a list of possible matches to pick from for an exact match.
- *[Shall/Should]* provide the ability to enter a misspelled street name and be presented with a list of possible matches based on SOUNDEX[6] and/or other methodology.
- *[Shall/Should]* provide the ability to enter an incorrect street address for a correct street name and be presented with a list of valid ranges.
- *[Shall/Should]* provide the ability to enter common street alias and abbreviations instead of the actual street name (*e.g.* MLK for Martin Luther King Blvd).
- *[Shall/Should]* provide the ability to override the CAD system's geofile by manually entering valid response area data.
- *[Shall/Should]* provide the ability to enter a reason for an overridden location.
- *[Shall/Should]* provide the ability to generate a report of geofile overrides.
- *[Shall/Should]* provide the ability to display the incident location in relation to other active incidents on the system's tactical map display during the CAD event entry process.
    - Data entry fields containing an address *[Shall/Should]* follow the *NENA Standard for NG9-1-1 GIS Data Model (71-003)*, Section 3.5 (GIS Database Model Layers) and should, at a minimum, include the data elements contained in the Site/Structure Address table.

Relevant Technical Standards / Guidelines

- *NENA Standard for NG9-1-1 GIS Data Model (71-003)*, Section 3.5, "Data Elements Contained in the Site/Structure Address Table" – In development[7]

2.11 Retrieve Incoming Calls



Incoming calls are typically answered in the order received, with priority given to calls from the 9-1-1 system. Non-9-1-1 calls are answered when no 9-1-1 telephone calls are pending. Larger PSAPs may use an Automatic Call Distribution (ACD) system, where priority calls are routed to the next available call taker and non-9-1-1 calls are also routed to an available call taker based on local PSAP policies. The PSAP's operating procedures will determine whether any call is allowed to go to voicemail or be put on hold.

[6] *Soundex* is a phonetic algorithm for indexing names by sound, as pronounced in English.
[7] Standard is in development by NENA. Visit http://www.nena.org/?page=Standards for more information.

As previously described, ALI data that contains the caller's specific location is presented to the call taker for landline and VoIP E9-1-1 calls. For wireless 9-1-1 calls, the ALI contains the caller's general location under WPH1 and a more detailed X,Y coordinate location under WPH2. ANI is provided for all incoming E9-1-1 calls, and possibly 9-1-1 and non-9-1-1 calls, depending upon how the system is designed.

CAD systems should be interfaced to the Customer Premises Equipment (CPE) to facilitate the automatic passing of ALI/ANI data to the CAD system. If the call taker has determined that the creation of a CFS is necessary, then the call taker should be able to initiate a CAD command via a command line, function key, mouse, or other method that results in the ALI data populating the CAD incident entry form with the location and call back telephone number of the reporting party. The call taker can then continue to collect and enter the remainder of the incident information available from the reporting party.

Most 9-1-1 telephone systems allow the call taker to *rebid*[8] a wireless 9-1-1 caller's current location when the system is utilizing WPH2 technology and the incoming call has been flagged as such. This feature is helpful if the caller is moving. The rebid feature will cause the ALI information to be refreshed with the reporting party's current location. It should be possible to, upon user command, import the updated location information from the telephone system into an appropriate area of the CAD event data entry screen.

Sample Requirements

In order to support the *Retrieve Incoming Calls* function, the CAD system:

- *[Shall/Should]* include an interface to the 9-1-1 telephone system that, upon user command, causes the automatic transfer of an emergency call's ALI information from the telephone system to an appropriate field of the CAD event data entry screen.
- *[Shall/Should]* allow call takers to initiate a CAD command/or function that will cause the CAD system to populate the CAD event data entry screen with call-back telephone number information if it is available.
- *[Shall/Should]* transfer, depending on PSAP policy, the telephone subscriber's name to a field in the CAD event data entry screen's reporting party's name data field.
- *[Shall/Should]* include data fields within the CAD event data entry screen for reporting party's name, address and callback number.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.12 Involved Person Information



The CAD system must be able to collect and display data about each individual involved in a CAD event. The information could be limited to only the name of the reporting party or a description of one or more suspects associated with a reported crime; however, the CAD system should provide the ability to capture a variety of data about individuals involved in CAD events, as well as the ability to search local databases to obtain any available information about these individuals,

[8] *Rebidding* is the process of re-querying the system for an updated location of a wireless 9-1-1 caller.

including: outstanding warrants, protection orders, mental or health issues, gang information, sex offender registry, and other advisory type information.

If the minimum required information is available for an involved individual, such as the gender, race, date of birth, and/or social security number, then appropriate inquiries to state and federal databases should be supported by the CAD system. These inquiries should be initiated upon user command and should require the user to manually re-enter the information already entered into the CAD system. CAD system users and responders should be able to initiate queries, either via desktop workstations or MDCs.

CAD query responses should be returned to the data entry originator. In the event that a subject is determined to be possibly wanted by law enforcement, the CAD system should audibly and visually alert both the emergency responder (if any) who originated the query or for whom the query was run, as well as the responder's controlling dispatchers.

The data entry operator will be able to add the returned information to the CFS and/or route the information to the responsible dispatcher and field unit MDC.

Sample Requirements

In order to support the *Involved Person Information* function, the CAD system:

- *[Shall/Should]* be capable of collecting the following information about each individual associated with an event:
    - Age
    - Date of Birth
    - Eye Color
    - Hair color
    - Height
    - Name
    - Operators License Number
    - Operators License State
    - Race
    - Sex
    - Weight
    - Additional remarks (*e.g.* clothing description, scars/marks/tattoos)
- *[Shall/Should]* initiate an automatic query, upon entry of information about an individual associated with an event, using the following guidelines at a minimum:
    - If the name only is known, then a name query *[Shall/Should]* be initiated to local files capable of performing a lookup based only on a name.
    - If the minimum required fields contain enough data for state and federal queries, then the system *[Shall/Should]* initiate queries to local, state and federal databases.
- *[Shall/Should]* return all responses from local, state, and federal databases to the data entry originator.
- *[Shall/Should]* bring positive responses (*e.g.* possible "hits") that require a review by the originator to the attention of the originator through the use of audible and visual indicators.

This requirement in no way supersedes federal and state regulations regarding access to criminal information, either from NCIC or a state's local database. NCIC and state portal access is and continues to be restricted to sworn law enforcement officers and those who have a direct need to know. Consult your state criminal information database administrator for more information.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.13 Involved Vehicle Information



The CAD system must be able to collect and display data about each vehicle involved in a CAD event. Support should be provided for information that is limited to only include a general description of the vehicle and a partial license plate; however, the CAD system should also support the ability to capture the variety of information typically required to fully describe a vehicle (*e.g.* make, model, primary color, secondary color, VIN, year). Once an involved vehicle is entered, the CAD system should be able to search local, state and federal databases to obtain and display all available information and alerts about the vehicle stored within them. The CAD system should support a cascaded query where, based on the registration response from the DMV, an additional query is generated to check for wants and warrants on the registered owners of the vehicle.

CAD system users (*e.g.* call takers, dispatchers, supervisors) and responders should be able to initiate vehicle queries either via their desktop workstations or MDCs. CAD query responses should be returned to the data entry originator. In the event that the vehicle is determined to be stolen or the vehicle owner has an outstanding warrant, the CAD system should audibly and visually alert both the emergency responder (if any) that originated the query or for whom the query was run and the responder's controlling dispatchers.

The data entry operator will be able to add the returned information to the CFS and/or route the information to the responsible dispatcher and field unit MDC.

Sample Requirements

In order to support the *Involved Vehicle Information* function, the CAD system:

- *[Shall/Should]* return all responses from local, state and federal databases to the data entry originator.
- *[Shall/Should]* bring positive responses (*e.g.* "hits") that require a review by the originator to the attention of the originator through the use of audible and visual indicators.
- *[Shall/Should]* be capable of collecting the following information about each vehicle associated with an event:
    - License plate
    - License plate state
    - License plate type
    - License plate year of expiration
    - Primary vehicle color

  - Vehicle Identification Number (VIN)
  - Vehicle make
  - Vehicle model
  - Vehicle year
  - Secondary vehicle color
  - Remarks

- *[Shall/Should]* initiate an automatic query to local, state and federal databases, upon entry of information about a vehicle associated with an event, using the following guidelines at a minimum:
  - License plate number and license plate state
  - VIN and vehicle make

- *[Shall/Should]* initiate a cascaded query, upon receipt of a response from the DMV containing the name of the registered owner of the vehicle, to local, state and federal databases, to check the wanted status, driver's license status, and other statuses of interest about the registered owner.

> This requirement in no way supersedes federal and state regulations regarding access to criminal information, either from NCIC or a state's local database. NCIC and state portal access is and continues to be restricted to sworn law enforcement officers and those who have a direct need to know. Consult your state criminal information database administrator for more information.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.14 Premises Hazards and Previous History



CAD must be able to store and display premises's hazards, tactical and previous CAD event information regarding the location of new CAD events. Hazard and tactical information about specific locations is collected and entered into CAD by field responders and communications center staff. The CAD system must provide appropriate data entry screens for entering this type of information and associate it with a specific address/location. Information about historical (previous) CAD events that occur at specific locations must be categorized by type and service agency, and automatically associated with a specific location/address by the CAD system. As events occur, and are processed, monitored and closed, CAD must keep track of them, store them, and associate them with the specific locations where they occur.

When a new CAD event is entered, the CAD system must search the location where the event is located and (optionally) neighboring locations to determine if previous events occurred there and whether any hazard or tactical information is available in CAD about the new event's location. CAD should display and alert users and responders about any premises and previous history information found at the new event's location. This information can include: occupant, premises or warning; previous incidents at the premises; whether the premises has records of registered firearms; hazardous materials stored at the

premises (usually business sites); serious medical information; wanted information concerning individuals residing at the premises; gated community and residential entry codes; Knox Box[9] location information; standpipe location information; special resource location information; and, other relevant alerts and safety information.

Related and/or additional relevant information could also be obtained via an interface to local RMS(s).

Sample Requirements

In order to support the *Premises Hazards and Previous History* function, the CAD system:

- *[Shall/Should]* have the capability to retrieve information about a premises and the surrounding/adjacent area as an automatic function during the creation of a CFS.
- *[Shall/Should]* have the capability to retrieve information about a premises and the surrounding/adjacent area as an ad-hoc query.
- *[Shall/Should]* display historical incident information based on a configurable date range pre-set by the systems administrator, and according to local SOP.
- *[Shall/Should]* display historical incident information based on a configurable geo-area range pre-set by the systems administrator, and according to local SOP.
- *[Shall/Should]* display historical incident information based on a configurable date range pre-set AND geo-area range pre-set by the systems administrator, and according to local SOP.
- *[Shall/Should]* be capable of storing information of interest to responders including, but not limited to:
    - Hazardous materials stored at the location
    - Firearms kept at the location
    - Information specific to individuals at the location, including, but not limited to:
        - Warrants on file
        - Serious medical information
        - Impairments
        - Potential dangers to first responders
    - Information specific to the address, including, but not limited to:
        - Entry codes
        - Knox Box information
- *[Shall/Should]* have additional fields available that are user definable.
- *[Shall/Should]* enable all required data for direct input, to be uploaded, or to be loaded via a live interface from RMS(s).
- *[Shall/Should]* be capable of integrating with a third-party syndromic alerting/tracking application.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

[9] A *Knox Box* is a small, wall-mounted safe that holds building keys for fire departments, EMS, and sometimes police to retrieve in emergency situations.

2.15 CAD Event Creation



CAD users must be able to create a new CFS event if there are no other active events in the CAD system for the same incident and location. A CFS event can be created by a call taker, dispatcher or responding resource depending on the source of the request. The CAD system must assign a unique incident/event number to each CFS event. Depending on local policies, the CAD system may spawn additional copies of the CFS event to facilitate the dispatch of additional services and agencies. Each copy of the CFS event must be assigned a unique incident/event number for the respective service or agency; however, it must also be possible to cross reference these CAD event records to each other in order to identify them as a unique system event.

Upon receipt of a priority event, the creator of the CFS must be able to enter the minimum mandatory amount of information required to create a CFS event (*i.e.* location and type of event), and to generate the CFS event. The CAD user must be able to forward that partially completed CAD event record to appropriate dispatchers so they are able to begin rolling emergency responders to the scene, while continuing to update the CFS event based on information obtained from the reporting party.

Sample Requirements

In order to support the *CAD Event Creation* function, the CAD system:

- *[Shall/Should]* support the creation of a CFS event with a bare minimum amount of information to trigger the dispatch of resources when the matter is urgent. This includes the location of the event and the event type.
    - It must be possible to update CFS event as additional information is gathered from the reporting party.
- *[Shall/Should]* support the creation of new CFS events—in communications centers where separate call takers and radio dispatchers are employed—by either call takers or dispatchers depending on the source of the event information.
- *[Shall/Should]* auto-create a CAD event for the Automated Secure Alarm Protocol (ASAP) standard if applicable. (See Section 2.17).
- *[Shall/Should]* spawn a copy of the CFS event—in agencies where multiple agencies and/or services are dispatched, or when an interface to another CAD system exists—for the additional agencies with a unique incident/event number for each; however, all copies of the CFS event *[Shall/Should]* be linked to each other so CAD users can ascertain that they are a single CAD event.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.16 Determining Response Agency and Service Area



The service agencies responsible for responding to an incident must be determined from the event's location. Often, the ESN information that arrives with E9-1-1 calls, or the WPH1 tower sector that received the call, specifies the agencies responsible for the call origination point; however, the caller's location is not always the location of the incident. Wireless calls often arrive with only either

a general X,Y coordinate representing the general area where a call originated (WPH1) or a detailed X,Y coordinate that represents the actual location of where the call originated (WPH2).

In either case, a point in polygon (PIP) or similar analysis must be performed to determine the service agencies responsible for the call's location but, again, the caller's location may not correspond with the actual event's location—therefore, the actual event location must be obtained from the caller and then validated against the CAD system's geofile to identify the law enforcement, fire, and EMS service agencies responsible for a new CAD event. The event type will help determine which service agencies must respond.

In order to assign field resources to a CAD event, the service area (*e.g.* fire response zone, police beat, EMS response area) must be determined. CAD systems must be able to use the event's validated location information (*e.g.* civic location, X,Y coordinate, street intersections) to determine the response area where the event is located for each service agency involved in the event.

Response areas and service agencies can be assigned in a variety of ways. Manual assignment can be made by call takers and dispatchers based on personal knowledge of an incident's location, manual look-up in a map book or wall map, street address table look-ups, or some other technique if an automated CAD system is not available. If a CAD system is available, then it usually uses its geofile to computationally determine the appropriate response areas and service agencies. Even if a CAD system with an excellent geofile is available, manual methods must occasionally be used in those situations where an event's geofile location cannot be validated or the location is ambiguous.

Sample Requirements

In order to support the *Determining Response Agency and Service Area* function, the CAD system:

- *[Shall/Should]* store all service agency and response area assignments in CFS events and the system's audit log file.
- *[Shall/Should]* validate the location of new a CAD event against the system's geofile to verify the location is within the service area handled by the PSAP.
- *[Shall/Should]* identify the new CAD event's location and nature code, and use the system's geofile to identify the appropriate service agencies that need to handle the event.
- *[Shall/Should]* identify the appropriate service agencies to handle a CAD event, and use the system's geofile to determine the appropriate response area(s) within each agency's service area.
- *[Shall/Should]* provide a method for CAD users to manually enter/assign the appropriate service agencies and response areas to CAD events if the CAD event's location cannot be validated against the system's geofile or if the validation process results in the assignment of an improper service agency or response area.
- *[Shall/Should]* use the service agency and response to notify the appropriate dispatchers that they must process a CAD event.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.17 Alarm Processing



Alarm monitoring companies are notified whenever an alarm monitored by the alarm company is triggered. A standardized alarm interface is available to digitally transfer the details of the alarms. Whereas some alarm monitoring companies are able to transmit the alarm details to the appropriate PSAP by using this standardized data exchange format, other monitoring companies must manually call the PSAP and verbally inform call takers of the nature of the alarm and its location.

When required by local ordinance, some CAD systems may include an alarm database that contains the ID (*e.g.* permit number or some other unique ID) along with the relevant information for that alarm. This database will enable the call takers to determine the nature of the alarm and whether it is a legal alarm simply by entering the ID number provided by the alarm company or via the alarm interface.

If an alarm interface is employed, then the entire alarm CFS event can be automatically created by the CAD system and routed to appropriate dispatchers without requiring any call taker interaction. Otherwise, the call takers either manually create the CAD alarm event or have the CAD system extract the information from the system's alarm database and forward it to the appropriate dispatcher(s) for responder assignments.

In those instances where communications centers are directly connected to alarm enunciator panels, their CAD system should either be directly connected to the panels so that a CFS event can be automatically created when alarms activate, or should include alarm tables that assist CAD users with the alarm CFS event creation process.

Sample Requirements

In order to support the *Alarm Processing* function, the CAD system:

- *[Shall/Should]* provide a feature where the location of an alarm can be retrieved by the number displayed on the enunciator panel, if the PSAP monitors alarm enunciator panels.
- *[Shall/Should]* adhere to the *APCO/CSAA 2.101.1-2008 External Alarm Interface Exchange American National Standard* (see below).
- *[Shall/Should]* receive alarm notifications and updates related to the alarm notification from alarm monitoring companies.
- *[Shall/Should]* utilize the alarm notification data to create a CFS event without call taker involvement if the address is valid and minimum required fields have been provided.
- *[Shall/Should]* spawn a copy of the CFS event to other agencies, if applicable.
- *[Shall/Should]* process updates from the alarm company as an update to the CFS and shown to the telecommunicator responsible for dispatch operations with an audible and visual indication that a new update has been received.
- *[Shall/Should]* send the appropriate response messages to each message received from the alarm company and enable system users to send update messages to the alarm company operator when additional information is required.
- *[Shall/Should]* send an automatic update message to the alarm company during the progression of the event—when the primary agency has been dispatched, when the primary agency has arrived on scene, and when the CFS has been closed, including any disposition information reported by the primary agency that responded.

Relevant Technical Standards / Guidelines

- APCO/CSAA 2.101.1-2008 *External Alarm Interface Exchange American National Standard* (Also-known-as: Automated Secure Alarm Protocol [ASAP]) – http://www.apcointl.org/911-resources/standards/apco-standards-for-download.html

2.18 CAD Event Routing



In PSAPs where one or more dedicated dispatch positions are employed, the CAD system must be able to route CFS events to appropriate dispatch positions after call takers have entered sufficient data for dispatchers to begin assigning and dispatching resources to the events. Typically, call takers and dispatchers need to work closely with each other—so the CAD system must be able to instantaneously (*i.e.* near real time) share new information entered into an CAD event records between all of the positions (call takers, dispatchers, supervisors, etc.) working the event.

Even though, communications centers may operate in a combined positions format where both the call taker and dispatcher are at the same position (telecommunicator), it is still desirable for the CAD system to be able to route CFS events and share information between positions—for example, law enforcement may arrive on the scene of an event and discover that fire and/or EMS resources are needed. The law enforcement dispatcher controlling the event must be able to route all of the relevant incident information collected to the appropriate fire and EMS positions without either position needing to manually re-enter any incident data.

Certain high priority incidents (cardiac arrest, bank robbery in progress, active shooting incidents, etc.) need to have emergency responders assigned and dispatched as quickly as possible. In these situations, as soon as the call taker obtains the incident type and validates the incident's location, the CFS event(s) must be transferred (routed) to the appropriate dispatch positions so that emergency responders can be assigned and dispatched; however, additional information collected after the routing takes place may be critical for dispatchers and responders to know. Also, the specific resource assigned, as well as other dispatch-related information about the event, may be required by call takers working the event; for example, the call taker may need to tell the reporting party: "Officer Jones is on his way and should be knocking at your door in a few minutes. Please continue what you're doing, but let him in when he knocks."

For these and other reasons, it is critical that all communications center personnel, as well as responders, have access to the latest information stored in CAD CFS events. This information must be routed between CAD positions and, if possible, out to emergency responders in the field, in as near to real time as possible.

CFS event routing can also involve a secondary PSAP, where CFS events are routed to a secondary PSAP via CAD-to-CAD or some other interface.

Sample Requirements

In order to support the *CAD Event Routing* function, the CAD system:

- *[Shall/Should]* examine the location, event type and response plans (when dedicated dispatch positions are in operation) to route the CFS event to one or more dispatch positions as the CFS event entry is being performed by a call taker.
- *[Shall/Should]* have a CAD-to-CAD interface for CFS routing to a secondary PSAP if the secondary PSAP operates its own CAD system independent of the primary PSAP's CAD system.

- *[Shall/Should]* display the dispatch position's pending event queue in priority order and in chronological order once the CFS event has been routed by the CAD system.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

2.19 Ability to Route to a "Decision Dispatcher"



This function addresses the business process where CAD events must be initially routed to a *decision dispatcher* before being routed to a dispatcher who will monitor and control the remainder of the incident. The decision dispatcher is aware of the location and status of all responder resources under his/her control, and, as such, is the only dispatcher to assign and dispatch resources to pending CAD events. Once the decision dispatcher alerts the assigned units/resources, the CAD system must route the CFS event to a radio dispatcher to handle the remainder of the event. Should additional resources be required for an event, then the decision dispatcher must be able to assign additional resources.

Typically, this function is implemented only by large fire and EMS communications centers. It is important to note that more than one decision dispatcher position may exist, and that the routing of the waiting event to the appropriate decision dispatcher may be based on incident/event type.

Sample Requirements

In order to support the *Ability to Route to a Decision Dispatcher* function, the CAD system:

- *[Shall/Should]* be capable of routing a CFS to a decision dispatch position that will dispatch resources.
- *[Shall/Should]* route the event (once the decision dispatcher has dispatched the event to the appropriate resources) to another dispatcher that takes responsibility for the event from that point forward.
- *[Shall/Should]* be able to route CAD events to the appropriate decision dispatcher (when multiple "decision dispatchers" exist) based on parameters configured by the system administrator.
- *[Shall/Should]* be able to route to the appropriate radio dispatcher (when multiple radio dispatchers exist to handle the remainder of the event) based on the actions by the decision dispatcher and/or predicated by event type and location.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3 DISPATCH SUPPORT

The dispatcher is responsible for using the CAD system in multiple ways to manage an incident. This section of the document will cover some of the most common and important features for a CAD system to assist the dispatcher in the dispatch decision and incident management process. Each section of the dispatch decision support function will be described in this section. This is not an all-inclusive list, but covers the most common areas of support.

Operational Examples

- *An 80-year-old male with chest pain* – The dispatcher will verify the location and may utilize a triage application to: determine the correct response plan; verify the recommended units have the correct capabilities and personnel attributes; select a radio channel to dispatch the units; and, alert the proper stations or units.
- *Chemical spill* – The dispatcher will: verify the location; select the correct response plan; verify the recommended units have the correct capabilities and attributes; select the proper radio channel; alert the proper stations or units; and, make appropriate additional notifications. If available, the dispatcher may also utilize a plume model and activate an emergency notification system.

3.1 Run Cards / Response Plans



A *run card/response plan* is a plan that identifies the number, type or specific units that respond to an incident of a specific type, and the order in which they respond. The plan also includes rules to allow for swapping units, or adding additional units if needed based on time or distance to the incident (*e.g.* if a unit was more than an allotted response time from the incident, the system might add a second unit of a different type to assist the first unit). Other concepts include: fixed run cards versus dynamic run cards; specification of alarm levels; and dynamic run cards aligned with AVL data and current unit status.

Run cards may be based on special criteria, such as: staffing capabilities, unit capabilities, secondary capabilities, personnel capabilities, resource groups, routing-based recommendations, target hazards, premises based response plans, response plans based on time of day or day of week, and other factors. Particularly in combined fire/EMS systems that use AVL, there is a need to define business rules for each incident/event type that control the order in which units are considered for dispatch, based on their locations relative to each other; for example, there may be a business rule to dispatch an Advanced Life Support (ALS) unit to a Basic Life Support (BLS) incident only if the ALS unit is at least 0.25 miles closer to the incident than the nearest available BLS unit. Many different types of business rules can be applied via the CAD system.

Sample Requirements

In order to support the *Run Cards / Response Plans* function, the CAD system:

- *[Shall/Should]* allow for dynamic and fixed/static response plans.
- *[Shall/Should]* allow for unlimited alarm levels.
- *[Shall/Should]* allow for the use of primary and secondary capabilities.

- *[Shall/Should]* allow for assignment to be by resource type, capability and equipment (*e.g.* thermal imager).
- *[Shall/Should]* allow for the use of personnel capabilities (*e.g.* personnel with Spanish speaking ability).
- *[Shall/Should]* allow for the use of resource groups made up of individual units [*e.g.* a Hazmat (hazardous material) group made up of several units and dispatched as a single "Hazmat team" (*i.e.* single unit)].
- *[Shall/Should]* allow for the use of premises-based or address-based response plans.
- *[Shall/Should]* allow for the use of AVL systems for selecting units.
- *[Shall/Should]* support multiple agency response plans.
- *[Shall/Should]* allow for unit assignment based on time or distance to the incident.
- *[Shall/Should]* allow for adjustable plans that are based on time of day or day of week.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.2 Adjustable Dispatch Levels



Adjustable dispatch levels refers to changing dispatch levels to alternative sets of dispatch policy plans in special circumstances, such as inclement weather, major incidents, disasters, Mass Casualty Incidents (MCIs), acts of terrorism, and low resource levels. Dispatchers should be able to raise and lower the level on demand; for example, a department has determined it needs to reduce response levels when activities consume 40 percent of all available resources within a jurisdiction. The first level of response reduction is to remove one engine company from a standard response complement. A higher level may be to remove two engines or an engine and a ladder company.

An example for law enforcement would be during special situations—an organized protest, special events (*e.g.* parades, large concerts), and higher than normal activity levels (*e.g.* roving gang warfare within an area)—normal dispatch responses may be increased or decreased based on adjustable dispatch levels; for example, a normal two-car response may be changed to a single-car response in a reduced dispatch level scenario—or, conversely, a normal one-officer/one-car response might change to a two-officer/two-car response if safety is an issue and the response level is raised.

In the EMS environment, instead of allowing the patient to choose the transport destination, the dispatch policy/response plan will dictate the patient be transported to the closest, most appropriate hospital; or, based on the information gathered during the EMD process, an ambulance may not be sent to the patient until after the special circumstances have diminished and adequate units are available for non-life threatening responses.

The consequence of changing the dispatch level is that the resource requirements change according to pre-defined response plans. The CAD system should allow for changing one or all of the response plans to a different dispatch level. There is a difference between changing the nature of the incident and changing the dispatch level since dispatch levels affect the entire agency response recommendations (*e.g.* a different set of events occurs when an EMS incident changes to a structure fire in the same location versus a structure fire in a location that is upgraded to a higher alarm assignment).

This item does not refer to changing the incident type, which could apply to law enforcement, fire, and EMS.

> Filling in the balance of an assignment (*i.e.* balance of alarm) that was only partially filled or adding units to the initial alarm is not the same as upgrading the alarm assignment (*e.g.* completing the balance of an incomplete first alarm assignment when transmitting a second alarm).

Sample Requirements

In order to support the *Adjustable Dispatch Levels* function, the CAD system:

- *[Shall/Should]* allow for adjustable dispatch levels.
- *[Shall/Should]* allow for an unlimited number of dispatch levels.
- *[Shall/Should]* allow for a user-defined naming convention for the dispatch levels.
- *[Shall/Should]* enable adjustable dispatch levels to be individually activated (*e.g.* a fire response plan would change to Level 2 and an ALS response would change to a Level 3, or all plans could change to a defined level).
- *[Shall/Should]* have an easily viewable method to review current dispatch levels.
- *[Shall/Should]* alert the dispatcher when the required number or type of units are not dispatched (*e.g.* one police unit to a domestic call instead of two, or two fire engines to a commercial fire instead of four).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.3 Additional Attributes



Additional attributes of units and personnel are needed to complement unit functionality. This information drives unit availability and recommendations for different incident types and events. The system should have the ability to allow dispatchers to modify the attributes on the fly and be dynamic. The system should also provide a way to search for attributes. Each unit should be able to have multiple unit and personnel attributes.

- *Examples of unit attributes include*: engine, ladder, aid car, medic, fire boat, patrol, Special Weapons and Tactics (SWAT), jaws of life/extrication equipment, rescue, key/battering ram, AR15, shotgun, Lo-Jack, Electronic Tracking System (ETS), Decon, power unit, Hazmat, K-9, dive, bomb squad
- *Examples of personnel attributes include*: communication, EMT/paramedic, ALS, SWAT, hostage negotiator, gang enforcement detail, mobile field force, mobile command center operator, Drug Recognition Expert (DRE), investigator, Spanish speaker, CISM

Sample Requirements

In order to support the *Additional Attributes* function, the CAD system:

- *[Shall/Should]* provide a means to assign multiple attributes to units.

- *[Shall/Should]* provide a means to assign multiple attributes to personnel.
- *[Shall/Should]* provide a means to search for units or personnel attributes on the fly.
- *[Shall/Should]* provide a means to assign resources to multiple units (*i.e.* shared crews).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.4 Mutual Aid Function



Fire and EMS dispatching is frequently based upon Memorandum of Understanding (MOU) agreements with other agencies such that the CAD system formulates resource recommendations based on another agency's resources, availability and location.

Mutual aid agreements are one type of MOU that dictates how CAD systems recommend resources for incidents located near a border between two or more agencies, or within a geographic area for which a mutual aid agreement is implemented.

Mutual aid agreements enable fire apparatus from one agency to respond to an incident located in a different agency's service area in the event of a major incident, or if the incident's location is physically closer to the neighboring jurisdiction's fire station. Similarly, a paramedic unit from EMS Agency X may be dispatched to an EMS incident in EMS Agency Y's service area because Agency Y's EMS unit is not available to respond or is too far away. Under a mutual aid agreement, cross-agency dispatching such as this normally requires that specific agency resources be designated as being "dispatchable" by a different agency. Before the resource can actually be dispatched, the requesting agency needs to manually contact (via radio or phone) the agency that owns the resource, explain the incident for which the resource is needed, inquire about the resource's availability, and request that it be dispatched to the incident. A real-time CAD-to-CAD interface may assist by transferring the relevant incident information from one agency to the other but, under mutual aid, the two agencies must still manually communicate with each other in order to actually dispatch the mutual aid resources.

Law enforcement resources from different agencies will also often respond to a single incident under informal or formal dispatch agreements when a major incident such as a robbery in progress, an active shooter, or similar incident occurs.

Inter-local and inter-agency mutual aid agreements between allied agencies can vary between jurisdictions and are subject to periodic change. A CAD system may include the ability to accommodate the variety of agreement terms and changes to terms that occur in existing agreements.

Examples of *configuration parameters*[10] include: the ability to indicate within which jurisdictions a unit can be suggested for dispatch as a mutual aid unit; whether or not the mutual aid unit is permitted to fulfill response requirements when suggested for dispatch into a particular jurisdiction (or needs to be backed up by another unit); and, when a mutual aid unit should be considered for suggestion (*e.g.* should be at least 0.5 miles closer than alternative units). This also includes defining sharing rules between units (*e.g.* an engine company might be able to respond only within its agency or the adjoining jurisdiction but not three towns over.)

[10] *Configuration parameters* are data variables and options that may be adjusted by authorized system administrators to control the behavior and response of a CAD system.

Many jurisdictions will refuse to share resources when their own resources fall below a certain level. Under these situations, the CAD system will suspend the usage of that agency's resources on incidents that would normally require the dispatch of that agency's resources to a different jurisdiction.

Sample Requirements

In order to support the *Mutual Aid* function, the CAD system:

- *[Shall/Should]* recognize the resources and capabilities of the host agency's own units and those of neighboring agencies.
- *[Shall/Should]* allow for custom mutual aid agreements, including business rules for utilization, and recognize various levels of response/mutual aid.
- *[Shall/Should]* recommend the use of other agency resources based on parameters within the mutual aid agreements.
- *[Shall/Should]* allow for redundancy and backup of the host agency's CAD system.
- *[Shall/Should]* auto-populate incident information (*e.g.* address information, nature of incident, resources needed) from other CAD systems via a CAD-to-CAD type interface.
- *[Shall/Should]* support the *Joint NENA/APCO Emergency Incident Data Document (EIDD)* or similar CAD-to-CAD functionality for sharing incident information as required for mutual aid agreements.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.5 Automatic Aid Function



Automatic aid agreements are a different type of MOU that control how fire and EMS resources are dispatched based upon agreements reached between one or more agencies. Under automatic aid agreements, the CAD system within one agency formulates resource recommendations based upon the location and availability of a different agency's resources. For incidents located near a border between two or more agencies or within a geographic area for which an automatic aid agreement has been established, the CAD system can recommend resources from the owning agency and/or from a different agency as long as the different agency's current resource status and location are available. Unlike with mutual aid, where manual communications are required to actually dispatch an allied agency's resources, under an automatic aid agreement, the resources can be automatically dispatched. Automatic, cross-agency dispatching such as this normally requires a real-time CAD-to-CAD interface, which enables the allied agencies' CAD systems to share incidents and resource availability and location information.

As with mutual aid agreement, inter-local and inter-agency automatic aid agreements between allied agencies can vary between jurisdictions and are subject to periodic change. A CAD system may include the ability to accommodate the variety of agreement terms and changes to terms that occur in existing agreements; however, unlike mutual aid agreements, automatic aid agreements enable the allied agencies to automatically dispatch each other's resources without requiring verbal communications. To support this capability, automatic aid agreements require that the status and location of affected

emergency resources be exchanged through a CAD-to-CAD type interface in an efficient and reliable manner between the CAD systems used by the allied agencies.

Examples of configuration parameters required for automatic aid agreements include: the ability to indicate within which jurisdictions a unit can be suggested for dispatch as an automatic aid unit; whether or not the automatic aid unit is permitted to fulfill response requirements when suggested for dispatch into a particular jurisdiction (or needs to be backed up by another unit); and, when an automatic aid unit should be considered for suggestion (*e.g.* should be at least 0.5 miles closer than alternative units). This also includes defining sharing rules between units (*e.g.* an engine company might be able to respond only within its agency or the adjoining jurisdiction but not three towns over.)

Automatic aid recommendations may be suspended when the owning agency's resources fall below a certain level. Under these situations, the CAD system needs to ignore automatic aid recommendations and only recommend its own agency's resources on incidents that would normally require the dispatch of a different agency's resources if the different agency's resources are depleted below the agreed upon level.

Sample Requirements

In order to support the *Automatic Aid* function, the CAD system:

- *[Shall/Should]* provide the capability to track the status (availability) of the host agency's own units and neighboring agency resources/units via a CAD-to-CAD type interface (*i.e.* overall view of unit resources).
- *[Shall/Should]* recognize the resources and capabilities of the host agency's own units and those of neighboring agencies.
- *[Shall/Should]* allow for custom automatic aid agreements, including business rules for utilization.
- *[Shall/Should]* recognize various levels of response/automatic aid.
- *[Shall/Should]* recommend the use of other agency resources based on parameters within the automatic aid agreements.
- *[Shall/Should]* allow for redundancy and backup of the host agency's CAD system.
- *[Shall/Should]* auto-populate incident information (*e.g.* address information, nature of incident, resources needed) from other CAD systems via a CAD-to-CAD type interface.
- *[Shall/Should] s*upport the *Joint NENA/APCO EIDD* or similar CAD-to-CAD functionality for sharing resource and incident information as required for automatic aid agreements.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.6 Unit Rotation (Unit Load Balancing)



Some departments require the ability to balance response loads among their resources; for example, in periods of high activity, run assignments may be adjusted by the CAD system to give rest to particularly busy units and to assign incidents to less active units. This is, in essence, *load balancing* response resources. The same is true for crews.

An engine company, for example, may be occasionally placed out of service or may only be considered available for dispatch based on predefined criteria (*e.g.* type of incident, priority of incident, proximity to incident relative to other units, etc.) in order to let that crew rest, while other, less busy, crews pick up their load.

Unit rotation/load balancing may also occur when more than one unit of the same type is housed in a single station, in order to balance the mileage or to prevent one unit from being over used.

Methods used for load balancing can vary from agency-to-agency and even station-to-station within the same agency, and may even differ based on type of incident. Preference may be given to:

- The unit with the older time of last dispatch;
- The unit with the fewest number of dispatches since the start of the shift;
- A particular unit based on the location of the incident; and/or,
- The time of day.

Some agencies utilize System Status Management (SSM), where predefined plans identify the most likely area that the incident will occur based on past history (*e.g.* historical, workload, calendar, day of week, time of day, etc.). The CAD uses these status management plans to recommend that units post themselves at specific locations in order to maximize coverage and minimize response times. The CAD system will continuously evaluate the status management plans, and will recommend unit relocations as other units respond to incidents or become available.

Sample Requirements

In order to support the *Unit Rotation* function, the CAD system:

- *[Shall/Should]* allow for customization based on the needs of the agency. (*e.g.* incident address, response type, assignment, resources required, unit-on-task-time, unit utilization, time of day and proximity if you have multiple available companies with the capability required).
- *[Shall/Should]* make unit response recommendations based on the configuration of rules defined by the agency.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.7 Conditional Availability of Apparatus



The *conditional availability of apparatus* function allows units with specific statuses to be recommended and dispatched to certain types of incidents; for example:

- A unit that is at the training center with hoses pulled may continue to be available for high priority incidents, but would not be recommended for routine incidents.
- A unit that is responding to a low priority incident (*e.g.* open fire hydrant, traffic congestion, lift assist) would be recommended for dispatch to a higher priority incident if closer than other units. The lower priority incident would be automatically re-queued for dispatch.

Sample Requirements

In order to support the *Conditional Availability of Apparatus* function, the CAD system:

- *[Shall/Should]* have the capability to code the conditional availability of units.
- *[Shall/Should]* be able to prioritize an incident and recommend the type of units based on the prioritization of that event and the current status of the unit.
- *[Shall/Should]* have a unit recommendation feature with the flexibility to be overridden by the dispatcher.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.8 Special Dispatch Areas



A *special dispatch area* is a geographic area for which a non-standard resource (*i.e.* unit) response is desired. The non-standard response may be permanent or temporary, and may apply only during specific combinations of days of the week and times of day. The geographic area may refer to one or more specific addresses, blocks, intersections, or arbitrary geographic regions.

Examples of locations where permanent special dispatch areas may be used are hospitals and schools. Examples of regions where temporary special dispatch areas may be used or that are more temporary in nature are flooded areas, restricted access areas, civil disturbances, and special events. Other CAD system functions may also be tied to these geographic areas (*e.g.* warnings displayed to dispatch personnel, warnings sent to responding units, automatically generated notifications).

Sample Requirements

In order to support the *Special Dispatch Areas* function, the CAD system:

- *[Shall/Should]* define special dispatch area types and assign each a unique identifier.
- *[Shall/Should]* assign a special dispatch area type to CAD geofile addresses, intersections, and blocks for each service agency (*e.g.* law enforcement, fire, EMS, utility).
- *[Shall/Should]* specify a non-standard response for a location identified with a special dispatch area type.
- *[Shall/Should]* define non-standard responses as being applicable only during certain days of the week and/or times of the day (*i.e.* window for utilization).
- *[Shall/Should]* provide the capability that if one or more windows are defined but none of them are applicable, then the standard response is employed.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.9 Emergency Medical Dispatch / Incident Triage



EMD or *incident triage* provides a set methodology for analyzing an event and determining an appropriate response based upon the information gained from the calling party. This capability guides the call taker through the process of collecting vital information from the caller, assigning incident status, choosing an appropriate dispatch level, and delivering approved standardized instructions to the caller until the appropriately dispatched unit(s) arrives at the scene. It may also provide pre-arrival instructions to responding unit(s) and the caller, as well as special dispatch instructions to help the dispatcher choose the correct resources. The EMD/incident triage process can result in a change to the incident type and/or response priority resulting in a change in the response. The CAD system may provide or interface with an EMD/incident triage product.

Sample Requirements

In order to support the *Emergency Medical Dispatch / Incident Triage* function, the CAD system:

- *[Shall/Should]* include (or allow for the installation of) an EMD or incident triage program.

The CAD system or EMD or incident triage program:

- *[Shall/Should]* allow for customization based on the needs of the agency (*e.g.* medical direction, operations).
- *[Shall/Should]* guide or prompt the call taker through defined forms based on the information provided by the caller.
- *[Shall/Should]* assist the call taker in identifying the:
    - Type of incident (*i.e.* law enforcement, fire, EMS, multi-agency)
    - Resources needed [*e.g.* law enforcement, ALS/BLS, engine(s), extrication]
    - Level of response (*e.g.* Alpha, Bravo, Charlie, Delta or priority)
- *[Shall/Should]* provide the capability to allow a unit to be dispatched to the incident as soon as the address is confirmed and the nature of the incident is determined.
- *[Shall/Should]* prompt the call taker to provide pre-arrival instructions to the caller or responding unit(s).
- *[Shall/Should]* recommend a change, based on the information obtained and entered into the program, in:
    - Response priority (*e.g.* upgrade or downgrade to emergent, non-emergent)
    - Resources required (*i.e.* law enforcement, fire, EMS)

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.10 Channel Designations



Radio channels and radio talk groups in a public safety environment are used for a number of purposes, including dispatching, records checks, and tactical incident management. Radio channels and talk groups used for tactical incident management are commonly referred to as *tac*

(*tactical*) channels.

Tac channels may be automatically assigned by the CAD system or manually assigned by a dispatcher. A CAD system should be able to recommend or automatically assign tac channels based on the incident type and agencies responding to ensure that the units' radios are all capable of communicating on the assigned tac channels. When an incident is cleared, any tac channels assigned to it are released. It is beneficial if there is an interface between the CAD system and the radio system that allows the CAD system to automatically switch the radios of those units assigned to the incident to the tac channel assigned to the incident.

Sample Requirements

In order to support the *Channel Designations* function, the CAD system:

- *[Shall/Should]* have a table of radio channels/talk groups.
- *[Shall/Should]* allow each radio channel or talk group to be used for tactical purposes to be flagged as such in the CAD system.
- *[Shall/Should]* allow each radio channel or talk group defined in the CAD system to have an associated list of the agencies whose units have those radio channels or talk groups on their radios.
- *[Shall/Should]* allow the radio channels or talk groups used for tactical purposes to be ranked according to the order in which they are assigned.
- *[Shall/Should]* track the maximum number of concurrent incidents that may be specified for each radio channel or talk group.
- *[Shall/Should]* include a flag indicating a requirement for the automatic assignment of a tac channel that can be set for each incident type in the CAD system.
- *[Shall/Should]* assign a tactical radio channel available to units upon the dispatch to an incident requiring the automatic assignment of a tac channel.
- *[Shall/Should]* allow the dispatcher to manually flag or assign one or more tactical radio channels or talk groups to an incident.
- *[Shall/Should]* track the release and reassignment of radio channels/talk groups.
- *[Shall/Should]* release the tac channels/talk groups assigned to an incident when that incident has been cleared and make the tac channels/talk groups available for other incidents.
- *[Shall/Should]* be able to, upon assignment of a tactical radio channel or talk group to an incident, direct the radio system to have the radios associated with units assigned to the incident to be automatically switched to that tac channel/talk group (if the radio system provides this capability).
- *[Shall/Should]* be able to, upon clearing an incident of which a tac channel/talk group has been assigned and the release of the channel or talk group has occurred, direct the radio system to have the radios associated with units assigned to the incident to automatically revert to their previous channel or talk group selection.
- *[Shall/Should]* be able to record which radio channels were patched together for an incident including start and end times.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.11 Be On the Look-Out / Attempt to Locate



A *Be On the Lookout* (*BOL or BOLO*), also-known-as an *Attempt to Locate* (*ATL*), alert can be a CAD function or a part of an RMS system; however, a BOLO should be accessible from either system based on the identifying name, address or hazard entered. BOLOs can be created and maintained in a table in the CAD system. BOLOs may be entered by a dispatcher or may be created by anyone who has been given the required security clearance to create or maintain the table.

Both an RMS interface and an MDC interface should support the creation and transmission of a BOLO back to the CAD system. A BOLO should be assigned an expiration date, either by the person who creates it or by the system, based on department policy and available system resources. A typical BOLO file would include the nature of the BOLO, priority, date, range of effectiveness, subject person information, subject vehicle information, hazards involved, and contact information. There should be a mechanism to search the BOLOs, to print them in a report, and to purge the BOLOs out of the date range. There should also be a mechanism in place to automatically notify the originating source of the BOLO anytime it is updated. Examples of a BOLO are:

- An unidentified white male traveling north in a red, Dodge minivan bearing Texas license plate ABC-123 may be in possession of stolen goods.
- That the same individual is operating the same vehicle with a major fuel leak, causing a safety hazard for both that individual and other commuters.

Sample Requirements

In order to support the *Be On the Look-Out / Attempt to Locate* function, the CAD system:

- *[Shall/Should]* support creation and distribution of any BOLO entered into the system.
- *[Shall/Should]* provide a BOLO structure to include all necessary information such as the nature of the BOLO, priority, date, range of effectiveness, subject and/or vehicle information, hazard information, and contact information.
- *[Shall/Should]* allow narrative fields for additional information.
- *[Shall/Should]* provide the means for BOLO information to be easily searchable, printable, and have the ability to automatically populate on an incident sheet referencing any particular name, address, or vehicle information.
- *[Shall/Should]* flag the field (automatically) with configurable visual and audible alerts.
- *[Shall/Should]* support a workflow record for initial BOLO creation and any additional edits.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.12 Dispatch Units



The units specifically recommended or selected for an incident will be dispatched and their acknowledgment recorded. All status changes associated with a unit's involvement with an incident should be recorded by the CAD system and become part of the CFS event. CAD systems should allow for documentation of times, via MDCs as documented by the responding personnel in their units, or by the dispatcher when the responding personnel verbalize their status via the radio (*e.g.* acknowledgement, en route, on scene, at patient, leaving scene, arrived at destination, back in service). Other units not dispatched may be notified of an event in-progress if the incident warrants. When multiple units are dispatched, one unit will be designated as the primary responder responsible for the incident until it is completed and any reports associated with it. Other units responding to the incident will follow the direction of the Incident Commander for the incident.

In the EMS environment, multiple patients may need to be treated and/or transported by multiple responding units and personnel. One unit will be primary and may function as 'Incident Commander' or 'EMS Incident Commander'. The National Incident Management System (NIMS) may be utilized so a Triage Officer, Treatment Officer, Transportation Officer, Staging Officer, and Safety Officer may also be needed.

Personnel skills and unit capabilities should be considered when units are recommended for dispatch. Based on the specific requirements of the incident, a unit or resource that is more appropriate may be assigned (dispatched) to the incident rather than the closest available unit. The CAD system will take into consideration the incident's requirements (*e.g.* nature/type, location, priority), the agency of jurisdiction's dispatch policies, and the skills and capabilities of the available personnel and units when recommending units for dispatch.

Sample Requirements

In order to support the *Dispatch Units* function, the CAD system:

- *[Shall/Should]* have the optional ability to assign one incident number to each unit responding to the incident.
- *[Shall/Should]* assign an incident number to each agency responding to the incident.
- *[Shall/Should]* assign, for an EMS response, a patient care report (PCR) number to each patient at the incident.
- *[Shall/Should]* capture every time stamp associated with each unit's response and status change related to the incident.
- *[Shall/Should]* capture all status changes and their times for statistical and research purposes (*e.g.* out of service versus in service to calculate "lost unit hours").

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

3.13 Resource Alerting



Units are notified that they have been dispatched to an incident, in a number of ways, in addition to the dispatcher advising them by using a

voice radio system. Additional information relating to an incident may also be relayed in ways other than by the dispatcher vocalizing the information. Such *resource alerting* mechanisms include:

- MDCs in public safety vehicles
- Radio system tone encoders that emit tones and then activate the public address (PA) system in a fire station or over an audio pager
- Fire station alerting systems that activate features in fire stations (*e.g.* lights, tones, PA systems, and message boards) and announces incidents
- Fire station "rip and run" faxes and printers that print out incident information
- Alerting via email delivered to portable devices
- Alerting via Short Message Service (SMS) delivered to cellular telephones
- Alerting via alphanumeric pagers using protocols such as TAP, WCTP, SMTP, and SNPP

Sample Requirements

In order to support the *Resource Alerting* function, the CAD system:

- *[Shall/Should]* alert via MDC.
- *[Shall/Should]* generate (automatically) information appropriate for use with "rip and run" printers and/or alphanumeric pager devices when units are dispatched or on demand by a dispatcher.
- *[Shall/Should]* generate (automatically) information appropriate for use with email and/or SMS sent to a mobile device when units are dispatched or on demand by a dispatcher.
- *[Shall/Should]* interface with tone encoder systems.
- *[Shall/Should]* interface with fire station, law enforcement, and EMS status and alerting systems.
- *[Shall/Should]* support "rip and run" printing via IP network using protocols, such as Internet Printing Protocol (IPP), Line Printer Daemon (LPD), and Hewlett-Packard Printer Job Language (PJL), and via facsimile transmission based on operational requirements.
- *[Shall/Should]* support alphanumeric paging via TAP, WCTP, SMTP, and SNPP.
- *[Shall/Should]* support sending SMS messages either directly via cellular modem or using a common carrier's SMTP interface.

Relevant Technical Standards / Guidelines

- Internet Engineering Task Force – http://www.ietf.org
    - RFC 1179: *Line Printer Daemon Protocol*
    - RFC 2821: *Simple Mail Transfer Protocol*
    - RFC 1861: *Simple Network Paging Protocol - Version 3 - Two-Way Enhanced*
    - RFC 2567: *Design Goals for an Internet Printing Protocol*
    - RFC 2568: *Rationale for the Structure of the Model and Protocol for the Internet Printing Protocol*
    - RFC 2910: *Internet Printing Protocol/1.1: Encoding and Transport*
    - RFC 2911: *Internet Printing Protocol/1.1: Model and Semantics*
    - RFC 3380: *Internet Printing Protocol (IPP): Job and Printer Set Operations*
    - RFC 3381: *Internet Printing Protocol (IPP): Job Progress Attributes*
    - RFC 3382: *Internet Printing Protocol (IPP): The 'collection' attribute syntax*

  - RFC 3510: *Internet Printing Protocol/1.1: IPP URL Scheme*
  - RFC 3995: *Internet Printing Protocol (IPP): Event Notifications and Subscriptions*

- International Telecommunication Union – http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx
  - *ITU-T T.4 Standardization of Group 3 facsimile terminals for document transmission*
  - *ITU-T T.30 Procedures for document facsimile transmission in the general switched telephone network*

- TAP - IXO – http://www.tap-ixo.info
  - *Telocator Alphanumeric Protocol Revision 1.8*

4 RESOURCE / UNIT MANAGEMENT

One of the fundamental and critical components of a CAD system is the ability to assign and track resources. Resources include not only the traditional responders—law enforcement, fire, and EMS—but may also include units like animal control, tow trucks, and utility services. Tracking of these resources is critical for the dispatcher to know what units are available to send to a particular CFS and what their status is at any given time.

Operational Examples

- A vehicle versus pedestrian accident with injuries call comes into the emergency PSAP. Reportedly, the pedestrian has life-threatening critical injuries. The dispatcher receiving the call from the call taker needs to assign resources—including law enforcement, fire, and EMS—as well as to place the medical transport helicopter on standby. The dispatcher relies on the CAD system to identify what units of each type are available and which ones are closest to the incident.

4.1 Move Up ("Fill-In" and "Station Fill")



Move up refers to the temporary reallocation or reassignment of one or more units in order to appropriately cover predetermined geographical response areas. This could be either automatically recommended by the CAD system or manually recommended.

> This functionality can occur from an interface with a third-party software program that decides coverage levels and recommends changes. As resource availability changes, the third-party software application may rescind a move up recommendation.

Sample Requirements

In order to support the *Move Up* function, the CAD system:

- *[Shall/Should]* recognize resource gaps that will likely result in response performance under prescribed standards.
- *[Shall/Should]* recommend or automatically dispatch units to move up to address those identified gaps.
- *[Shall/Should]* initiate move ups based on user defined manual or automated logic processes.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.2 Staffed vs. Unstaffed Units



Volunteer fire and EMS agencies may require CAD system functionality that supports the ability to handle unstaffed units as available. This also applies to combination (*i.e.* career and volunteer) and paid on-call departments. In the case of paid/on-call, this functionality can assist in

tracking hours of on-call resources. It is also helpful for tracking specialized groups such as Hazmat, SWAT, and Urban Search and Rescue (USAR) teams.

CAD systems track units are staffed with specific numbers of people; however, in some circumstances, units may need to be documented as unstaffed to show the time a unit was dedicated to an incident and then unstaffed—for example, a pumper truck that was delivered from one agency to another and left to pump water in order to fill brush pumpers. Special response units or tactical vehicles may also need to be tracked as they are assigned for stand-by in certain situations. Vehicles can also be assigned a particular parameter or at a facility to show a visual sign of security and, therefore, need to be tracked as a resource but not necessarily as man hours.

Sample Requirements

In order to support the *Staffed vs. Unstaffed Units* function, the CAD system:

- *[Shall/Should]* provide the ability to dynamically document that a unit is staffed or unstaffed before or after it is assigned to an incident.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.3 Cross-Staffing / Crew Counting / Shared Staffing / Contingent Staffing



Cross-staffing can be either station-based or unit-based:

- In *station-based cross-staffing*, crews can jointly staff more than one available unit. When the crew level (generally the number of personnel available in quarters) is reduced to less than needed for the remaining unit or units, the units in quarters are placed out of service.
- Unlike station-based cross-staffing, *unit-based cross-staffing* is a one-to-one relationship. When one unit responds, the cross-staffed unit is placed out of service. Multiple units may be shared.
- *Crew counting* is based on minimum unit staffing (*e.g.* two medics required for a unit to respond with ALS capabilities). Additional units may need to be dispatched to meet a minimum certification level, skill set, and/or equipment set.

Sample Requirements

In order to support the *Cross-Staffing* function, the CAD system:

- *[Shall/Should]* account for the number of qualified personnel available in a station, and determine the best possible resource allocation from that station at any given moment.
- *[Shall/Should]* utilize any combination of dedicated or contingent staffing to most appropriately utilize resources.
- *[Shall/Should]* account for the qualifications of personnel—such as fire apparatus driver/operator, EMS certification, and rescue certification—to establish the best possible resource allocation based on prioritized needs for the response.

- *[Shall/Should]* take, based on a single shared crew assigned to multiple pieces of apparatus, the remaining piece(s) of apparatus out of service, when one piece of apparatus is assigned to an event.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.4 System Status Management (Dynamic Resource Deployment)



SSM is the practice of strategically pre-positioning resources to minimize response times. Resources may be positioned at permanent or temporary post locations (*e.g.* street corners). The CAD system should have the ability to build system status plans (by hour of day, day of week, etc.) that define the levels of resource availability and what posts/stations should be prioritized for coverage. For example, if only one ambulance is available in the system at 2:00 p.m. on weekdays, then that unit might be positioned in the center of a city. In this example, that post would be the "Priority 1 Post." The plan should be able to accommodate multiple priority posts in each plan, and posts may be designated as equal to or alternates to other posts in the plan.

The CAD system should continually monitor each plan in effect for the current time period and alert the dispatcher if the plan goes "out of compliance" (*e.g.* units are not in their proper positions). The CAD system may allow users to view the out of compliance condition, and provide a recommendation to the dispatcher for how to position units to meet the requirements of the plan. The dispatcher will be able to accept, override or ignore CAD recommendations. For AVL enabled systems, vehicle location would be used in SSM.

The CAD system provides the capability for multiple plans by unit resource type; for example, there may be separate ALS and engine SSM plans. As resource levels change (*e.g.* units are assigned to incidents, clear off incidents, come on shift or go off shift), the plan will automatically update.

The SSM function may be provided via a third-party interface. The CAD system can generate SSM-related performance metric reports.

This functionality can be provided via an interface with a third-party software program.

Sample Requirements

In order to support the *System Status Management* function, the CAD system:

- *[Shall/Should]* build multiple system status plans (*e.g.* by hour of day, day of week) that define the levels of resource availability and which posts/stations *[Shall/Should]* be prioritized for coverage.
- *[Shall/Should]* monitor, on a continuous basis, each plan in effect and alert the dispatcher if the plan goes "out of compliance" (*i.e.* units not in their proper position).
- *[Shall/Should]* include the capability for multiple plans by unit resource type.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.5 Additional Unit Status



Minimal time tracking that may be included in CAD systems include status changes such as: received, dispatch, en route, arrived on scene, patient contact made, transport, transport complete, and cleared.

As law enforcement, fire, and EMS services rely heavily on the CAD system's ability to track resources and response times, additional unit status functionality is required to track resource availability. The following is a list of such statuses that should be considered:

- *Assigned to Post/Move Up*— This would be a designated stand-by location either predetermined or dynamic and based on incident activity and better readiness for response.
- *En Route to Post*
- *At Post*
- *Available in Area of Assigned Post*
- *Available for Emergency Incidents Only*—This can be used when a unit has released the patient and can respond, but is working on paperwork, stocking supplies

Unit statuses that relate to the tracking of units that are assigned to incidents or allow for the tracking of patients need to be also included. The unit statuses that are employed by CAD systems include:

- *Staged*—This would document being in the area of the incident and waiting for approval to proceed to the scene of the incident.
- *Patient/Incident Contact*—This would be a secondary on scene time that tracks when stand-by stops and contact is made on the incident.
- *En Route to Hospital*—Transporting could also be used but specific information needs to be included, such as dynamic destinations, which may include specific hospitals or long term care facilities.
- *At Hospital*—Transport complete could also be used for this status.
- *Clear From Hospital*—This may be used when a unit becomes available but has not arrived back in its coverage area.

Some unit statuses may also be needed to support modifiers, as shown in the table below.

TABLE 3. UNIT STATUS MODIFIERS

STATUS	MODIFIER 1	MODIFIER 2
En Route	• Without lights and siren; or, • With lights and siren	• Available for dispatch; or, • Unavailable for dispatch
En Route to Hospital	• Without lights and siren; or, • With lights and siren	• ALS patient; or, • BLS patient

Sample Requirements

In order to support the *Additional Unit Status* function, the CAD system:

- *[Shall/Should]* include the various statuses needed for unit readiness or during patient care.
- *[Shall/Should]* add parameters to the incident that relate to the response priority (*i.e.* lights and siren or non-emergency mode).

- *[Shall/Should]* show if a unit is BLS or ALS.
- *[Shall/Should]* allow for multiple transports by the same unit on the same incident (*e.g.* a mass casualty incident).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.6 Strike Team / Task Force Designations



Law enforcement, fire, and EMS organizations require a CAD system to have the ability to create *strike teams* and *task forces* that can be designated as *virtual units*. Strike teams or task forces are groups of predefined units or "on-the-fly" groups that respond and operate together during large-scale events. The resources need to be individually tracked within the database but need to be grouped during the event for ease of tracking and response.

Task forces and strike teams are temporary complements of resources designed to be deployed in special circumstances; for example, in wild land firefighting, a task force of three engine companies and an ambulance may be assigned to fight a fire on a ridge as a single unit. Rather than the CAD system accounting for, dispatching and tracking the individual units, the engine companies and ambulance are grouped "on the fly" by the CAD system and collectively managed. SWAT or tactical teams are good examples of law enforcement strike teams.

Once grouped into a strike team or task force, individual units are not normally considered for independent dispatch. The task force may also include units that are not included in day-to-day operations, or that are pre-set prior to deployment. These units could include mutual aid units that fill a need of the task force, such as a tanker truck or a triage team from the local hospital.

Sample Requirements

In order to support the *Strike Team / Task Force Designations* function, the CAD system:

- *[Shall/Should]* allow the dispatcher to group units into a task force or strike team (*i.e.* virtual unit).
- *[Shall/Should]* track (individually) all resources in the system's database, and *[shall/should]* also make a record that the resources were part of a virtual unit so the virtual unit response data can be easily retrieved.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.7 Rostering



Rostering is the process of assigning personnel for a shift or partial shift to a vehicle or position. Rostering allows users and dispatchers to place units on-duty with the scheduled and nonscheduled personnel when they report for duty. Units may be automatically brought on and off duty at

differing times or locations.

Roster records should include the portable radio ID, pagers and other equipment specific to that unit or the personnel staffing the unit. Units should also be able to be placed on duty on-the-fly if they are coming in for an emergency shift that was not previously scheduled. The system should allow the unit to be placed off duty at the end of the shift, if desired, and should record the duration of the shift for reporting. The CAD system should allow personnel modifications during the shift in the event a crew member goes home sick and is replaced or should allow other changes, such as a shift exchange. The system should allow rostering of additional personnel above the normal crew complement (*i.e.* additional crew members, volunteers or observers). The system should also warn when a unit has inadequate personnel whether in numbers or skill set qualifications. A CAD system will be able to manage this as either an internal or interfaced function with an external product.

Sample Requirements

In order to support the *Rostering* function, the CAD system:

- *[Shall/Should]* provide the capability to create rosters (*i.e.* assign personnel to a vehicle or position to facilitate on/off duty transactions).
- *[Shall/Should]* allow the dispatcher to adjust the rosters and/or assignments (*i.e.* on-the-fly, during shifts, and above normal complements).
- *[Shall/Should]* warn the dispatcher if a resource complement is below minimum.
- *[Shall/Should]* contain a 2-way, real-time interface to auto populate roster information in CAD.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.8 Scheduling



Scheduling is the process of assigning personnel to a designated shift, platoon, beat that repeat in a logical pattern. The CAD system should recognize scheduled personnel and their assignment, and should appropriately roster them. Scheduling is dynamic and frequently changes. Scheduling should reflect the agencies' work codes, and should accurately represent the staffing of the department. A CAD system should be able to manage workforce scheduling as either an internal or interfaced function. Scheduling includes routine platoon rotation as well as overtime, exchange of shift, and special call-outs.

Sample Requirements

In order to support the *Scheduling* function, the CAD system:

- *[Shall/Should]* provide scheduling capabilities to include pre-assignment of personnel to shifts, platoons, beats
- *[Shall/Should]* allow the dispatcher, with proper permissions, to make adjustments to scheduling on-the-fly and/or during shifts.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.9 Mileage Tracking



For billing and other purposes, agencies may require the ability to track mileage on each incident. For EMS, this would be used for billing; for fire, for response efficiency analytics; and, for law enforcement for tracking the transport of subjects.

Sample Requirements

In order to support the *Mileage Tracking* function, the CAD system:

- *[Shall/Should]* capture beginning and ending mileage for individual transports.
- *[Shall/Should]* provide a visual and audible error indication to the user upon failure to enter beginning or ending mileage based on transport or response type.
- *[Shall/Should]* provide a method of integration with an AVL system for increased accuracy and efficiency.
- *[Shall/Should]* use GIS/mapping to supplement driving directions based on shortest route beginning and ending address locations, with regard to environmental factors such as time of day, weather conditions, train schedules, and road/bridge blockages.
- *[Shall/Should]* include the use of intuitive interfaces that facilitate mandatory entry based on given incident types or processes.
- *[Shall/Should]* provide an interface to billing and reporting components.
- *[Shall/Should]* provide the ability for an authorized user to manually override an entry by a dispatcher or supervisor.
- *[Shall/Should]* record the overridden information in an audit log.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.10 Hydrant Location and Status



The hydrant location and status capability allows CAD to track the location, service status, most recent test date, and/or flow rate/main size of fire hydrants and alternative water sources (*i.e.* drafting sites, dry hydrants, pools, and ponds). Hydrant recommendation should be displayed to dispatchers and responders based on location of the incident. Hydrant information may be obtained from an external GIS source. This should be displayed on the approach route system map and should allow the user to drill down into this information from the mapping window. Hydrant data should also be automatically displayed to the incident responders on their MDC or on a station printout when the unit is alerted. When a hydrant is placed out of service, the system map and MDC should clearly display that information. The CAD system should also generate a report indicating all hydrants that have been placed out of service with appropriate dates.

This functionality can be provided via an interface with a third-party software program.

Sample Requirements

In order to support the *Hydrant Location and Status* function, the CAD system:

- *[Shall/Should]* track fire hydrants, including: location, service status, recent test date, flow rate, and main size.
- *[Shall/Should]* display hydrant locations and related info on the map.
- *[Shall/Should]* indicate (automatically) the closest hydrants to fire calls for service.
- *[Shall/Should]* record, and display, with hydrant information, alternative water sources (*e.g.* ponds, creeks).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.11 Additional Unit Dispositions



A *unit disposition* records an action made by a single unit with respect to a specific incident. When a unit transitions from active status (*i.e.* assigned to a specific incident) to available status at the end of the incident, a dispatcher may assign a disposition from a pre-defined list to that unit, along with a comment or note. This results in the unit's action regarding the incident to be recorded at the time that the unit completes its work at an incident. For example:

- One of two engines en route to an incident is cancelled before arriving on scene. The cancellation places the engine in an available status and can be assigned to another incident.
- Two ambulances arrive on scene and one transports while the other does not transport. Individual unit dispositions may be independent of the incident disposition.
- Multiple law enforcement units respond to an incident. Agency policy may require that one of more dispositions be recorded on a per unit basis.

Units that are equipped with a MDC should be able to enter their own dispositions without dispatcher involvement.

Sample Requirements

In order to support the *Additional Unit Dispositions* function, the CAD system:

- *[Shall/Should]* enable the CAD administrator to define a list of available unit dispositions.
- *[Shall/Should]* require a disposition based on call type and jurisdiction.
- *[Shall/Should]* enable assisting units to report one or more dispositions when agency policy requires a disposition from each unit assigned to a CFS.
- *[Shall/Should]* facilitate the recording of dispositions by the dispatcher or the field unit if MDC-equipped.

- *[Shall/Should]* include a multiplication factor for each disposition when multiple instances of the same disposition apply (*e.g.* 10 traffic summons written could be recorded using a single disposition of "traffic summons issued," times 10).
- The CAD system *[Shall/Should]* NOT require a disposition if agency policy does not require the use of dispositions.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.12 Exception Reason Tracking



The CAD system should allow dispatchers to record reasons when a unit has an extended response time that exceeds the standard. The CAD system tracks response time standards for each priority and each jurisdiction and prompts the dispatcher to enter a "late reason" when the incident is completed or at the end of their shift. Exception reasons can be pre-defined and relevant comments can be added.

Sample Requirements

In order to support the *Exception Reason Tracking* function, the CAD system:

- *[Shall/Should]* identify and require an exception in any case when user defined response time standards are not met.
- *[Shall/Should]* establish a system administrator-defined list of exception reasons established for each CAD time interval.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.13 Public Safety Flight Tracking



This addresses the ability to track aircraft flights. There are Federal Aviation Administration (FAA) and Commission for the Accreditation of Air Medical Transport Systems (CAAMTS) requirements to follow aircraft in flight for specific time periods. This may be provided by an interface with an external flight following system. This function typically does not use the drive-time algorithms used in ground-based operations, but rather "as the crow flies."

Sample Requirements

In order to support the *Public Safety Flight Tracking* function, the CAD system:

- *[Shall/Should]* adhere to the FAA and CAAMTS requirements, if required by agency policy.
- *[Shall/Should]* have an interface access to, and be able to record, flight weather.

Relevant Technical Standards / Guidelines

- Commission on Accreditation of Medical Transport Systems – http://www.camts.org

4.14 Geo-fencing



Geo-fencing refers to the function of providing alerts when automated location systems report resources entering or leaving a geospatially-defined area. Current technologies support geospatial reporting from numerous devices, including radio units, vehicles and cellular devices. The ability to alert, record and play back these actions is critical to operations, operations review and post action support.

Sample Requirements

In order to support the *Geo-fencing* function, the CAD system:

- *[Shall/Should]* provide geo-fence creation tools that allow the use of polygons, circles, ellipses, and rectangles.
- *[Shall/Should]* display details about a resource to aid in identification, location and purpose.
- *[Shall/Should]* facilitate the creation of multiple, coexisting, overlapping geo-fences.
- *[Shall/Should]* support unique geo-fence names and each geo-fence *[Shall/Should]* be visually distinct.
- *[Shall/Should]* generate an alert whenever a vehicle or resource enters and/or exits a geo-fence.
- *[Shall/Should]* include alerts that consist of:
    - Unique visual and audible identification
    - Resource identification
    - Geo-fence Identification
    - Current resource position
    - Timestamps of entry and exit of geo-fence areas
    - Ability to clear alerts and history from view while maintaining historic records as needed
- *[Shall/Should]* include standard GIS functions, such as exportation of parcel Information, data fields, and historic records from geo-fence in agency based required formats.
- *[Shall/Should]* be able to alert personnel though technologies such as text messaging or email.
- *[Shall/Should]* provide the ability to create, manage and record geo-fence areas to track the entry and/or exit of GIS based resources.
- *[Shall/Should]* provide informative and manageable alerts to appropriate personnel through visual and audible representation.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.15 Station Dispatch



Station dispatch refers to the function of dispatching a station rather than specific units to an incident. An example would be dispatching a rural volunteer fire department station to a motor vehicle crash; if no response is confirmed by the station that was dispatched, then a unit from a nearby

jurisdiction would be dispatched.

Sample Requirements

In order to support the *Station Dispatch* function, the CAD system:

- *[Shall/Should]* provide the capability to dispatch a fire and/or EMS station to an incident regardless of the number of units or personnel that station has assigned to it or on duty.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.16 Pre-Release or Pre-Alerting



Pre-release, or *pre-alerting*, refers to the function of providing advance notice to stations and/or units that an imminent dispatch is likely to occur. These functions are used when enough information has been gathered to know that some type of dispatch will be required. The pre-release/pre-alert allows the dispatcher to notify units to prepare for a response and reduce turnout time. In some cases, units may begin to respond or arrive on location before the CFS event is dispatched.

Sample Requirements

In order to support the *Pre-Release or Pre-Alerting* function, the CAD system:

- *[Shall/Should]* provide pre-release or pre-alert functionality to alert stations and units to new incidents and the corresponding address and/or location prior to the CFS event being dispatched.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.17 Vehicle / Unit Change



This functionality addresses the ability of the CAD system to change, on the fly, and in any status mode, the identity of a unit based upon a change in the unit's staffing, capability, status, or resources. Included in this requirement is the ability to transfer a unit's capabilities from one unit to another. This includes transferring all radios, pagers, and MDCs.

Sample Requirements

In order to support the *Vehicle/Unit Change* function, the CAD system:

- *[Shall/Should]* account for the number of personnel currently staffed on the unit.
- *[Shall/Should]* allow system supervisors and other authorized users the ability to modify vehicle and resource capabilities, as required, without adversely impacting the system (*i.e.* without having to shut the system down).
- *[Shall/Should]* allow easy modifications to unit crew capabilities to accommodate frequent changes throughout the day.

- *[Shall/Should]* track units having multiple units with multiple capabilities, and attributes *[Shall/Should]* be reflected as multiple types (*e.g.* a Quint, pumper, or ladder).
- *[Shall/Should]* recommend resources based on the appropriate type (*e.g.* a "Quint" type fire apparatus may be recommended as either a pumper or a ladder truck).
- *[Shall/Should]* allow the dynamic entry of personnel staffing specific units/apparatus.
- *[Shall/Should]* allow the staffing module to be accessed from the field by authorized users to dynamically reflect changing assignments.
- *[Shall/Should]* allow for tracking vehicle ID in addition to unit radio call sign (*e.g.* a given vehicle may be referred to as "Unit 1" one day and a different vehicle the next day.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.18 Automatic Driving Directions / Routing



Automatic routing is the service provided by a CAD system to advise units of the best route to respond to an incident, based upon the responding unit's current location. Routing should take into consideration any road closures or other relevant information stored in the CAD system.

Sample Requirements

In order to support the *Automatic Driving Directions / Routing* function, the CAD system:

- *[Shall/Should]* present the destination address visually for validation and acceptance.
- *[Shall/Should]* provide a route that considers current impedances (*e.g.* road closures, road construction, accidents, disable vehicles)
- *[Shall/Should]* provide a route that considers speed limits, traffic lights, stop signs, and other traffic control variables.
- *[Shall/Should]* provide a visual map that presents the entire route.
- *[Shall/Should]* provide a visual map that centers the unit and presents a configurable radius around the unit (*i.e.* feet, miles, meters), and provides turn-by-turn navigation.
- *[Shall/Should]* provide consistent route re-evaluation, and visually present alternate routes based on estimated drive time without interfering with current route.
- *[Shall/Should]* provide a directions list from unit current location to destination.
- *[Shall/Should]* present visual and audible warnings about travel impedances.
- *[Shall/Should]* allow authorized field units to create and clear impedances, which may be used for directing other units.
- *[Shall/Should]* account for one-way roads, highway overpasses, and other considerations that impact safety.
- *[Shall/Should]* include traffic weights that are considerate of time-of-day, day-of-week, and day-of-year to account for rush hour and holiday congestion.

- *[Shall/Should]* store suggested route and route taken for future evaluation.
- *[Shall/Should]* provide configurable forms that allow resizing, on-off, and night/day modes.
- *[Shall/Should]* provide configurable audible alerts and voices that can be enabled and disabled.
- *[Shall/Should]* provide a manual entry interface for non-CAD driven use.
- *[Shall/Should]* prevent audible alerts from interfering from other system notifications that may impact unit safety.
- *[Shall/Should]* allow for tracking of train schedules/locations that result in blocked crossings.
- *[Shall/Should]* allow for tracking of train AVL data to factor blocked crossings.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.19 Bypassed Units



For CAD systems that use AVL, dispatch personnel should be notified when a closer appropriate unit becomes available for dispatch to an incident to which another unit has already been dispatched; for example, if Engine 4 was out of service when an incident was dispatched in its assigned area and the unit that was dispatched to the incident is still further from the incident than Engine 4 when Engine 4 goes back into service, appropriate dispatch personnel are notified of Engine 4's possible availability.

Sample Requirements

In order to support the *Bypassed Units* function, the CAD system:

- *[Shall/Should]* alert (automatically) the dispatcher in the case of a unit becoming available that is closer to a CFS in which the currently assigned unit is still in route and farther away.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

4.20 Post-Dispatch Response Re-evaluation



For CAD systems that use AVL, dispatch personnel should have the ability to reevaluate the appropriateness of the units assigned to an incident. The CAD system should notify the dispatcher when a reevaluation is appropriate. The reevaluation should indicate to the dispatcher, based on current unit locations and status:

- Any units that should be added to the incident;
- Any units that should be cancelled; and,
- Any units that could be cancelled if the units indicated have been added to the incident.

For example, when dispatch personnel are notified that a unit that had been bypassed on an incident is now available, this feature would be used to indicate to the dispatcher that Engine 4 should be added to the incident and that the other unit could be cancelled after Engine 4 is added.

Sample Requirements

In order to support the *Post-Dispatch Response Re-evaluation* function, the CAD system:

- *[Shall/Should]* notify the dispatcher when a response reevaluation is appropriate based on AVL data (*i.e.* units that should be considered for a CFS and units that could be cancelled if those under consideration are assigned to the event).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5 CALL / INCIDENT / EVENT MANAGEMENT

The incident is managed by continually updating the CFS event with any additional information reported by callers or officers on scene. The resource recommendations may be revised based on additional information and may be added to or reassigned.

Operational Examples

- An original CFS is a structure fire and a fire unit is on the scene. The fire is growing, so the assigned unit requests additional fire units and traffic control. The dispatcher requests a "second alarm recommendation" from the CAD system, so the system provides recommended, additional fire units based on proximity, unit type and availability. The dispatcher also creates a request for a law enforcement unit for traffic control.
- Law enforcement is responding to a hit and run accident. A second call-taker is on the phone with a witness who is in a car and following the suspect. The second call-taker is routinely providing updates to the CFS event regarding suspect location and description. The dispatcher is relaying this information to responding units as it is added to the record.

5.1 Display of Incident / Event Data



The CFS will be queued to the dispatcher for processing. Upon selection, all entered information for the incident will be displayed to the dispatcher. This will include map data, response information, premises history information, and other supplemental information, such as known hazards and wanted persons. Some of this information may be available through the use of window tabs, where the information can be retrieved and viewed based on the needs of the dispatcher.

As updates are entered via the call taker, another dispatcher or field units, the displayed CFS event will be automatically updated to include this new information. An audible and/or visual indication is provided to the responsible dispatcher on the CAD screen once a CFS event is updated.

Immediate access to all open CFS events (including unassigned) are provided on the CFS status display.

When a CFS event is closed, it will be automatically removed from the CFS event display. Separate windows or window tabs may exist for unassigned events, assigned events, and all events.

Sample Requirements

In order to support the *Display of Incident / Event Data* function, the CAD system:

- *[Shall/Should]* display CFS event data on the CAD monitor after being selected by the dispatcher. All CFS event data *[Shall/Should]* be accessible to the dispatcher.
- *[Shall/Should]* enable Windows tabs to be used to allow the dispatcher to select supplemental history about the incident (*e.g.* premises history, past event history, hazards, persons of interest)
- *[Shall/Should]* display (automatically) updates to the CFS event for the dispatcher.
- *[Shall/Should]* provide updated information that is easily discernible from the previously read data (*e.g.* newest information on the top, different font/color text).

- *[Shall/Should]* present an audible and/or visual indication to the dispatcher when a CFS event is updated by another source such as a call taker, another dispatcher, or a field unit.
- *[Shall/Should]* provide, upon receipt of an update, a method of ease, such as an 'Update' button, for the dispatcher to retrieve the CFS event that has been updated.
- *[Shall/Should]* remove CFS events as they are closed by the dispatcher from the CFS event display, without additional interaction from the dispatcher.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.2 Update Incident Status



If no additional information is required (*i.e.* the resource requirement is unchanged, supplemental resources are not needed), then the status of the incident is updated as new information is received. This should include updating the reported incident type to the actual incident type; for example, once the immediate incident is resolved, the responding unit will communicate to the dispatcher that the scene is secured.

> In some jurisdictions, dispatchers may not always make the decision as to whether the event has adequate resources. In those instances, it is most likely an incident commander on scene that makes this determination and the dispatcher will respond accordingly.

Sample Requirements

In order to support the *Update Incident Status* function, the CAD system:

- *[Shall/Should]* provide the capability to record supplemental information updates in the CFS event as it is received from callers, field resources and other sources.
- *[Shall/Should]* retain a copy of any information updated prior to the update for audit purposes.
- *[Shall/Should]* provide a method to update the actual incident type versus the reported incident type.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.3 Dispatch Resource Decision



If the resource requirement is changed, then the system will recommend resources that will be assigned based on existing procedures that factor the workload and unit capability with regard to skills and equipment required for the incident, unit availability, and the proximity of resources.

Sample Requirements

In order to support the *Dispatch Resource Decision* function, the CAD system:

- *[Shall/Should]* recommend resources, when the resource requirement is changed, based upon agency defined procedures, workload balancing, unit capability, and proximity of the resources.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.4 Update Assigned Resources



If changes to the assigned resources are needed, then the updated recommended response complement should be adjusted and recorded based upon predetermined criteria.

Sample Requirements

In order to support the *Update Assigned Resources* function, the CAD system:

- *[Shall/Should]* detect when a reduction in dispatched resources is required.
- *[Shall/Should]* recommend readjusted resources that meet the requirements of the incident.
- *[Shall/Should]* record the modifications to the CFS event when changed by the dispatcher.
- *[Shall/Should]* record any changes to assigned resources as an update to the CFS event.
- *[Shall/Should]* provide the capability to recommend additional resources based on response plans and/or local policies.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.5 Update Supplemental Resources Tracking



When supplemental resources are needed, the CAD system will be able to track these resources and provide recommendations based on user-defined criteria.

In cases where a vehicle has been confiscated or found to be disabled, the dispatcher needs the ability to request the services of a towing company. This request may be made by company name (owner requested) or by rotation. In cases where the vehicle owner does not have a preferred company, the system will select a company from the towing rotation list. A towing rotation prevents any one company from being favored over another. Other examples utilizing this functionality could be locksmiths, private ambulance transport companies, and taxis.

If resources other than those recommended by the rotation are selected, then the system will capture the reason for the exception.

Sample Requirements

In order to support the *Update Supplemental Resources Tracking* function, the CAD system:

- *[Shall/Should]* allow the ability to divide the response area into multiple zones, based on user-defined criteria, to ensure a quick response to the request.
- *[Shall/Should]* make recommendations for resources to prevent any one entity from being favored.
- *[Shall/Should]* allow cancellation of or by-passing the recommendation, returning the skipped company to be placed back in the rotation either at the bottom or top of the rotation, depending on the circumstances.
- *[Shall/Should]* provide the ability to skip a suggested resource, capturing the reason for the exception and placing the resource either back at the top of the queue or at the bottom, based on the reasoning.
- *[Shall/Should]* provide the ability to create and maintain rotating and non-rotating service provider information (*i.e.* towing companies).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.6 Assign Units



The dispatcher will assign responders to an incident based on the incident type, location and user-defined response criteria. Units assigned to the incident will have their unit histories reflect the dispatch and any further action taken while assigned to the incident. The CFS event will also be updated with all unit IDs assigned to the incident and any changes in their statuses during the incident.

The dispatcher will relay pertinent information about the incident to the dispatched units in the field. An optional MDC interface supports this activity as well.

Based on priority levels and the resource needs of the incident, units assigned but available to other incidents may be pulled off of the current assigned status to handle a higher priority incident. If all units are pulled off of an incident, then the CFS will be added back into the dispatch queue to be re-dispatched when resources are available.

Sample Requirements

In order to support the *Assign Units* function, the CAD system:

- *[Shall/Should]* allow the assignment of units by using drag-and-drop and point-and-click pull-down menus.
- *[Shall/Should]* re-queue the CFS that has had all units removed, but has not been handled.
- *[Shall/Should]* recommend a unit that is unavailable *only if* SOP permits units to be pre-empted for a higher priority event.
- *[Shall/Should]* provide the ability to assign one or more units to an incident with a single command.

- *[Shall/Should]* provide the ability to dynamically, and without user intervention, change the unit recommendation if relevant incident information changes (*i.e.* type, location, alarm level).
- *[Shall/Should]* provide the ability to notify users that the unit recommendation has changed.
- *[Shall/Should]* provide the ability to cancel a unit from an assignment: If the cancelled unit is the only unit assigned, then the CFS will be returned to the pending event queue.
- *[Shall/Should]* provide the ability to assign or add multiple units to a CFS event with a single command.
- *[Shall/Should]* provide the ability to assign a single unit to multiple CFS events.
- *[Shall/Should]* provide the ability to hold a CFS event for a specific unit.
- *[Shall/Should]* allow the dispatcher to override the system recommended units and assign other units.
- *[Shall/Should]* allow the dispatcher to assign any valid field unit to an incident even if that unit is not currently logged on to the system.
- *[Shall/Should]* notify the dispatcher and confirm that the correct unit has been assigned if a unit assigned to an incident is not logged on the system.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.7 Update Incident Data



Additional details about an incident may be received from various sources (*e.g.* public safety responder, citizen, resource searches). Information related to an incident will be added to the CFS event and submitted to the controlling dispatcher for processing as information becomes available. The receipt of additional information may result in re-classification and re-prioritization of the incident.

The call taker and dispatcher will need the ability to enter narrative data at any time prior to and after closing the incident. For documentation validation, all entries into the CFS event should be time stamped with the date/time the information was entered or modified.

As multiple callers provide potential witnesses to the incident, and may provide additional or supportive information, documenting their information is pertinent to the investigation process.

Sample Requirements

In order to support the *Update Incident Data* function, the CAD system:

- *[Shall/Should]* log the following information for all entries into the CFS event: date, time, user ID (or note if action was system generated), position (terminal) ID, action performed, and any notes associated with action.
- *[Shall/Should]* display additional CFS event information to the dispatcher for action.
- *[Shall/Should]* allow, at any time, additional incident information to be added to the CFS event, both prior to and after closing the incident.
- *[Shall/Should]* allow the user to display the added comments in reverse chronological order.

- *[Shall/Should]* provide the user the option of specifying the CFS event to update by entering the call sign of any assigned unit or by entering the incident number.
- *[Shall/Should]* permit multiple users, including MDC-equipped field resources, the ability to simultaneously update information to the CFS event.
- *[Shall/Should]* provide controls when two or more CAD users attempt to update the same field in the CFS event
    - For example, in the event that User A is saving modifications to a field, and that field has been modified by another user since User A retrieved the CFS event, the application *[Shall/Should]* notify User A that the field that is being modified has been changed since User A retrieved the record and confirm that User A wants to continue with the update.
- *[Shall/Should]* provide the ability for one or more CAD users to simultaneously add incident information to an active or closed CFS event.
- *[Shall/Should]* provide the ability to add supplemental information to closed incidents based on assigned user rights.
- *[Shall/Should]* notify the entering party that the incident being updated has been closed. This will allow the entering party to reopen the incident for re-queuing to dispatch if necessary.
- *[Shall/Should]* provide the ability to update the CFS event by specifying the incident/event number or the call sign of assigned units.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.8 Assign Records Management System Incident / Case Number



In addition to the CAD system incident/event number, an RMS incident number or case number may be assigned to the incident for tracking purposes. When serving multiple jurisdictions, the need for transfer of information may vary by agency. The CAD system allows RMS incident number assignment based on individual agency policy. The assignment of the RMS number may happen at any time, but usually occurs upon incident closure. The RMS number may be assigned from a table of incident numbers maintained in the CAD system in coordination with the RMS system or through an interface with the RMS system. In some environments, the RMS incident number can be the same as the CAD event number. The CAD system incident number process is configured according to agency policies.

Sample Requirements

In order to support the *Assign Records Management System Incident / Case Number* function, the CAD system:

- *[Shall/Should]* facilitate an interface to an RMS to allow the transfer and tracking of incident data.
- *[Shall/Should]* provide the ability to transfer the incident data to the RMS at a set time (incident closure) or at dispatcher discretion based upon the field unit's needs.

- *[Shall/Should]* coordinate the assignment of RMS incident/case numbers through a jointly used, shared list by the RMS and CAD system or through a list maintained in the CAD system.
- *[Shall/Should]* provide the ability for the dispatcher to retrieve the RMS incident number at any point during the event or after the incident has been closed.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.9 Transfer Basic Incident Data to the Records Management System



If agencies choose to transfer data from the CAD system into an RMS, then the specific fields and amount of data can be set based on agency needs. Normally, incident data gets transferred to the agency for use by the records section in an editable format.

The following are examples of the types of data found in an incident report:

- CAD incident type
- Date/time of incident
- Details of incident
- Disposition codes
- Location of incident
- Report number
- Units assigned to incident

The CAD system incident/event number is included to provide a cross-reference between the CFS event and the subsequent RMS incident report.

Transfer to an RMS of CFS event data associated with the incident is normally triggered and automatically takes place as an agency-specific report number is assigned at the time of final disposition of the incident. The CAD system will have a feature whereby administrative commands can be executed to transfer the CFS data associated either with a specific incident or a series of incidents based upon parameters.

The CAD system will allow an earlier transfer of the data to obtain the agency-specific report number when requested by the public safety responder. Depending on the transfer functionality, if an earlier transfer is prior to incident closure, not all data fields may transfer.

Depending on agency policy, sometimes the CAD incident/event number is used as the RMS incident/case number.

> It is assumed in this document that the Fire Records Management System supports the submission to the National Fire incident Reporting System (NFIRS) and that CAD supports NFIRS by providing what information it can (as appropriate) to the fire RMS.

Sample Requirements

In order to support the *Transfer Basic Incident Data to the Records Management System* function, the CAD system:

- *[Shall/Should]* provide the ability to automatically transfer CAD system CFS event data relating to an incident to an RMS for use by the agency.
- *[Shall/Should]* provide the ability to transfer data prior to the normal chronological transfer point to provide the public safety responders with an RMS incident number when needed, and if this method is required to retrieve an RMS incident number.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.10 Display Additional Incident Data



As additional information is made available, the dispatcher will be alerted and have the ability to view the new information within the CFS event (*e.g.* any information entered by a call taker, another dispatcher, or a field unit).

The system will provide a notification for each entry completed, as this will ensure the dispatcher is made aware of each entry for processing. When multiple entries are made for the same incident, the information will be displayed with the most current information on top. This will ensure the dispatcher is aware of the most recent developments first.

Sample Requirements

In order to support the *Display Additional Incident Data* function, the CAD system:

- *[Shall/Should]* notify the appropriate CAD users via visual and/or audible indication when information is added or changed to a CFS event.
- *[Shall/Should]* provide a separate notification for each entry made.
- *[Shall/Should]* provide the ability to visually differentiate text notes in the CFS event added by different operators for the same incident (*i.e.* color and/or CAD user identification).
- *[Shall/Should]* display additional CFS event data with the newest information displayed first.
- *[Shall/Should]* display additional CFS event data with the newest information displayed in differently formatted text (*e.g.* color, font, formatting, such as bold, italics).
- *[Shall/Should]* provide the ability to view all additional CFS event data at one time.
- *[Shall/Should]* provide the ability to automatically notify users monitoring or displaying the CFS event that information has changed.
- *[Shall/Should]* provide the ability to dynamically, and without user intervention, display changes to a CFS event as they occur based on assigned user rights.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.11 Reopen Incident



When additional information is added to a closed CFS event, the person entering the data will be notified that the CFS event has been closed.

At this point, the person entering the additional data, if allowed and appropriate, can re-open the CFS event for re-processing. If a field unit is notified that the CFS event is closed, then the unit may need to contact a dispatcher to re-open the CFS event on its behalf. Call takers can re-open CFS events, but are normally not allowed to close CFS events, depending on agency policies.

Any changes are time/date stamped for audit purposes.

Sample Requirements

In order to support the *Reopen Incident* function, the CAD system:

- *[Shall/Should]* ensure all changes to the CFS event are time/date stamped.
- *[Shall/Should]* notify the CAD user attempting to add information to a closed CFS event that the event is closed.
- *[Shall/Should]* provide the ability to add comments to a CFS event without reopening the original CFS event.
- *[Shall/Should]* provide the ability to reopen a CFS event by incident number, location, or unit ID.
- *[Shall/Should]* provide the ability to reopen closed CFS events and assign units.
- *[Shall/Should]* provide the ability to open a closed CFS event as a new CFS using information from the old CFS event, but with new time stamps.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.12 Add Destination Locations



On occasion, a single incident will involve numerous "destination locations" (*e.g.* multiple hospitals, facilities, jails, detoxification centers, half-way houses). The CAD system should have the ability to capture multiple hospital or facility destinations of units transporting patients or clients. This information can be captured at multiple points during the incident within the CFS event. Additionally, a law enforcement agency may desire to record the destination for a prisoner transport.

Sample Requirements

In order to support the *Add Destination Locations* function, the CAD system:

- *[Shall/Should]* have the ability to accurately track the destination of all units assigned to a particular incident within the CFS event, and to allow these locations and activities to change throughout the incident.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.13 Hospital Status / Availability and Hospital Recommendation



Hospital Ambulance Diversion

Hospital ambulance diversion refers to the tracking of hospital availability/status (*i.e.* available, busy, closed) within the CAD system. The system may also provide a warning to units if transporting to a closed or non-recommended facility. The hospital status may also be a routing instruction; for example, an emergency room may be under construction and the ambulance may need to use an alternative entry point.

From time to time, the resources of a hospital may become taxed. In an effort to provide optimal patient care, a hospital may request that patients by ambulance be diverted to another facility so that care may be expedited. In doing so, many times this places an undue responsibility upon the pre-hospital provider and a burden upon the patient.

Because hospitals are able to exercise a certain amount of control over patients being transported by ambulance, they are able to inform pre-hospital personnel of their status and go on diversion.

The CAD system may include a dedicated, secure Internet access allowing hospitals to exchange status and other information to support daily and crisis operations. The system incorporates many features to support patient planning assumptions on a regional and statewide basis. The secure, password protected website is designed to be updated daily by all hospitals, assuring that hospitals will use this critical resource in an emergency situation. This system allows hospitals to update status in real-time and at a time convenient to the hospital. This assures a common tool for all hospitals to collect and disseminate critical information during a significant disaster event. Its use on a daily basis assures that hospitals are familiar with the Web page and can access it during the time of crisis.

Hospital Bed Availability

For purposes of estimating institutional surge capability in dealing with patient disposition during a large mass casualty incident, the following *hospital bed availability* estimates also may be reported:

- *24-hour Beds Available*—An informed estimate of how many staffed, vacant beds for each category above could be made available above the current number within 24 hours. This would include created institutional surge beds, as well as beds made available by discharging/transferring patients.

Hospital Recommendation

Hospital recommendation refers to the system recommending the appropriate hospital based on geography and/or capabilities, such as the closest hospital, a hospital with the appropriate specialized facility (*e.g.* burn unit, trauma center), or the hospital that is next on the rotation. The system provides a warning to units if transporting to a closed or non-recommended facility. This could be an interface with external systems.

Sample Requirements

It may be prudent to consider a third-party application interface so the information is accessible outside of the CAD system network.

In order to support the *Hospital Status / Availability and Hospital Recommendation* function, the CAD system:

- *[Shall/Should]* track hospital diversion status and hospital bed availability, and provide hospital transport recommendations.

Relevant Technical Standards / Guidelines

- American College of Surgeons: *Guidelines for Ambulance Diversion* – http://www.acep.org/content.aspx?id=30038
- OASIS: *Emergency Data Exchange Language (EDXL) Hospital Availability Exchange (HAVE) v1.0* – http://docs.oasis-open.org/emergency/edxl-have/v1.0/errata/edxl-have-v1.0-os-errata-os.html

5.14 Patient Tracking



In any large-scale disaster with multiple victims, emergency responders use a triage system to evaluate each patient's injuries, prioritize treatment, and provide transport to medical facilities for those who need it. There is a need for the ability to track the movement of patients from the scene through hospital discharge. A patient tracking system will facilitate that process for emergency responders and hospitals. Emergency responders on the scene of a mass-casualty incident need to efficiently and accurately track the number of injured, as well as the status and location of each victim.

The ability to track patients removed from the scene to their ultimate destinations or disposition is of significant importance. This functionality includes the ability to maintain data on multiple patients and multiple destinations. This could be an interface with a third-party software package. The system may be capable of assisting the dispatcher to track and list patients based on information transmitted by radio, phone or other technology. The system will maintain a database of patient identifying information, such as: name, age, gender, primary medical complaint, date of birth, ambulance or other transport unit number, hospital, or other destination/disposition.

Sample Requirements

The tracking platforms *[shall/should]* be compatible and interoperable with other appropriate systems.

In order to support the *Patient Tracking* function, the CAD system:

- *[Shall/Should]* have the ability to track EMS patients from the scene to their destination or disposition.
    - This *[Shall/Should]* include the ability to capture patient identifying information.
- *[Shall/Should]* meet Federal HIPAA (Health Information Portability and Accountability Act) requirements for data security where appropriate.

Relevant Technical Standards / Guidelines

- *ANSI/HIBC 1.3-2010* – http://www.hibcc.org/Standards/ANSI%20HIBC%20%20PAS%201.3%20FINAL_errata.pdf
- *The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules* – http://www.hhs.gov/ocr/privacy/
- OASIS: *EDXL-Tracking of Emergency Patients (TEP 1.0)* – In development[11]
- OASIS: *EDXL-Tracking of Emergency Clients (TEC)* – In development[12]

5.15 Linking an Audio File to a CAD Event



Audio logging, also referred to as *recording*, is a significant component in the PSAP technology infrastructure. This is the act of recording forms of audio and video in a PSAP such as: the 9-1-1 telephone call, radio system, console-to-console intercom, administrative lines, NG9-1-1 video, CAD screens, ANI/ALI, and direct connect ring down telephone lines.

The ability of the CAD system to associate a CFS event record with the captured audio for that incident is imperative during the Quality Assurance (QA) process and for rebuilding the scenario that occurred. This functionality is also required when reconstructing an event for public disclosure requests and/or court cases.

As NG9-1-1 is still being developed, other incoming media types will need to be included in this process as they are introduced.

> This function could be contained within a CAD system or provided via a separate recorder device interfaced with the CAD system for the purpose of linking the recording to a particular CFS.

Sample Requirements

In order to support the *Linking an Audio File to a CAD Event* function, the CAD system:

- *[Shall/Should]* provide the ability to record multiple types of incoming media types and associate them with the CAD CFS event record for easy retrieval.
- *[Shall/Should]* provide the ability to add additional types of data to this association as they are developed.
- *[Shall/Should]* provide the ability to associate a CAD incident with audio logging/recording.
- *[Shall/Should]* allow the user to open a window to support streaming multimedia feeds (*i.e.* video and audio).
- *[Shall/Should]* allow users to start, stop, pause, and rewind the multimedia feed.
- *[Shall/Should]* allow for adequate start/stop capabilities.

[11] Standard is in development by the OASIS Emergency Management Tracking of Emergency Patients Subcommittee. Visit http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency-tep for more information.
[12] See above.

  - If the multimedia feed is stopped or paused for less than 30 seconds and then restarted, then the multimedia feed *[Shall/Should]* start where the stop or pause occurred.
  - Stopping or pausing the data stream for up to 30 seconds *[Shall/Should]* not cause the loss of the data.
  - There *[Shall/Should]* be at least a 30-second cache of the multimedia data stream.
- *[Shall/Should]* allow multimedia data to be recorded into CFS event history; or, otherwise allow the recording of streaming media to a separate data repository with appropriate information that would allow the users to easily match multimedia files with specific incidents.
- *[Shall/Should]* allow authorized users to start/stop the recording process by the use of graphic command buttons or function keys.
- *[Shall/Should]* support the resizing of the multimedia window and the auto-resizing of the video display portion of the window.
- *[Shall/Should]* interface with a separate audio recording device to include linking a CFS to the appropriate recording(s).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.16 Multiple Simultaneous Incidents to Single Unit



This refers to the ability to assign multiple incidents to a single unit. Commonly referred to as *stacking* or *held incident*, it provides a method of assigning multiple low priority incidents to a single unit and allowing the unit to either pick from the assigned batch of CFS events or to automatically receive information for the next incident upon closing the current incident. Although units can be assigned multiple simultaneous incidents, they can only act on one incident at a time. The data for each incident is stored within the CFS event used by the system.

This capability is well suited for certain calls within each responders group:

- Law enforcement community policing activities where patrol officers handle all low-priority issues within their patrol area;
- Fire department responses to high volumes of automatic fire alarms, wires-down, or outside fires associated with wide-spread weather conditions; and,
- EMS for public service wellness visits.

If this capability is used, controls should be in place to avoid incidents being assigned to a unit, but then subjected to prolonged response times. The dispatcher may need to monitor the overall incident loading on various units and re-allocate to other available units when required.

Pre-emption during an incident is different from stacking, as a *pre-empted* incident occurs when the only assigned unit is removed from the incident due to re-assignment. If the incident is pre-empted, then the CFS event needs to return to the CFS event pending queue so the dispatcher can assign another unit.

Units are typically not diverted. Diversion of a unit to another event could equate to a pre-empted CFS event if the diverted unit is the only unit assigned.

Multi-agency incidents can be linked so they retain their agency-specific incident numbers and CAD system incident types; however, all associated unit status, updates, and ancillary information are recorded in all CFS event and incident records.

Holding means that events are in the pending queue and not yet assigned because they are being held for a specific unit.

Sample Requirements

In order to support the *Multiple Simultaneous Incidents to Single Unit* function, the CAD system:

- *[Shall/Should]* allow a dispatcher to hold or stack events to a busy unit, as well as units that are in-service.
    - If a unit is on an assignment, when the unit clears its assignment, then the system *[Shall/Should]* notify the dispatcher the unit is available.
- *[Shall/Should]* provide the agency a method to define what events can be held.
- *[Shall/Should]* notify the unit that it is being held when an event is placed on hold.
- *[Shall/Should]* allow several events to be placed on hold for a single unit.
- *[Shall/Should]* allow a CFS event to be held for a unit that is not yet logged on.
- *[Shall/Should]* record in the history of the CFS event when an event is placed on hold.
- *[Shall/Should]* apply timers to all held CFS events and alert the dispatcher when a held event has exceeded the allowable time in a held status.
- *[Shall/Should]* provide dispatchers with the ability to pre-empt a unit and dispatch the unit to another event.
    - If all units are removed from the original event, then it *[Shall/Should]* be placed in the pending CFS events monitor.
- *[Shall/Should]* NOT limit the ability of the dispatcher to assign another unit to the incident or for field units to self-dispatch (assign) themselves to an event that has been placed on hold, if permitted by agency policy.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.17 Scheduled Events



Scheduled events are events scheduled in the CAD system for some time in the future, such as a controlled burn, non-emergency hospital transports, a fireworks display, or funeral escorts. Scheduled CFS events will be automatically placed in the pending queue a certain number of minutes prior to the start time to allow the dispatcher to assign resources in advance. There may be other details necessary in the call taking function for scheduled incidents to ensure the appropriate resource is assigned.

Sample Requirements

In order to support the *Scheduled Events* function, the CAD system:

- *[Shall/Should]* provide the ability to automatically schedule the CFS event for future dispatch.
- *[Shall/Should]* allow scheduled events to be created by entering a CFS or by sending a message.
- *[Shall/Should]* be capable of displaying a list of all scheduled events.
- *[Shall/Should]* provide the ability for authorized users to activate a scheduled event at any time.
- *[Shall/Should]* send a message to the appropriate users when the scheduled activity occurs.
- *[Shall/Should]* support location override for scheduled incidents.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.18 Secondary Incident Location



This refers to the ability of the CAD system to capture, validate and track units that are assigned to the same incident but operating at different locations from the primary or initial location. This is frequently used in law enforcement when a crime occurs at the incident location but a suspect is at another location. Similarly, fire units may be assigned to different locations on scene of a large fire. Units are able to be assigned various status designations at the secondary location.

Sample Requirements

In order to support the *Secondary Incident Location* function, the CAD system:

- *[Shall/Should]* provide the ability to note responding apparatus has arrived "in staging," which may be a remote secondary address associated with the primary incident location.
- *[Shall/Should]* provide the ability to change a unit's location from the primary address to a secondary address without clearing the unit from the incident or CAD record.
- *[Shall/Should]* log a date/time stamped record of the change in the CFS event.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.19 Single Discipline Incident to a Combined Discipline Incident



This addresses the ability for the dispatcher to add agencies to an existing incident by creating unique incident/event numbers for the added agency and transferring existing incident data to the newly-created CFS event record(s). Inter-agency events are linked and automatically share pertinent information, such as narratives and address changes.

Sample Requirements

In order to support the *Single Discipline Incident to a Combined Discipline Incident* function, the CAD system:

- *[Shall/Should]* provide the ability to add another agency's resources to a CFS event.
- *[Shall/Should]* provide the ability to assign an agency specific incident/event number to the CFS event.
- *[Shall/Should]* provide the ability to link added agency records with the initial CFS event.
- *[Shall/Should]* provide the ability to share incident information across multiple linked records.
- *[Shall/Should]* provide the ability to track the added resources for the duration of the incident.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.20 Timers



Fire/EMS functionality will require additional timer functions, such as failure to respond (*i.e.* if a first unit is dispatched and does not respond, a timer alerts the dispatcher to move to next due unit). Additional timers might include extended time at a scene or a hospital.

For law enforcement, timers are an officer safety issue; for example, alerting the dispatcher to an overdue check-in on a traffic stop. Timers may be "connected" to or based on the CAD incident type (*e.g.* every 3 minutes during a traffic stop; every 5 minutes for a drunk and disorderly; or, every 15 minutes for a larceny report).

System timers allow for alerts for such things like a call taking too long to have a unit assigned to an incident (non-dispatched).

Sample Requirements

In order to support the *Timers* function, the CAD system:

- *[Shall/Should]* have, and allow configuration of, multiple timers based on unit status and CAD incident type, such as time on a particular call, time since last check-in, and time at the hospital or jail.
- *[Shall/Should]* have, and allow configuration of, timers for CAD system events, such as a priority 1 call overdue to be dispatched.
- *[Shall/Should]* allow for operators to manually place a timer alert on a CFS or a unit.
- *[Shall/Should]* minimally include "down to the second" timestamps (*e.g.* hhhh/mm/ss).
- *[Shall/Should]* allow configurable timers (*i.e.* 'hh:mm:ss', 'mm:ss', or 'ss').

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

5.21 User Defined Status Timers



Additional timers are needed to accommodate fire/EMS functionality. These include: incident duration checks, crews operating in Immediately Dangerous to Life or Health (IDLH) environments[13], Personnel Accountability Report (PAR) checks, time in environments, time in rehabilitation, burn time, patient contact time, and other user-definable status timers. Systems offer predefined timers, as well as the availability of reserved fields for user definable timers. This function may also be applied to law enforcement for officer safety checks during self-initiated incident/events.

Sample Requirements

In order to support the *User Defined Status Timers* function, the CAD system:

- *[Shall/Should]* be equipped with predefined timers that can be configured by the system administrator.
- *[Shall/Should]* provide the ability for the system administrator to create customized definable timers.
- *[Shall/Should]* record timer activity to the CFS event log.
- *[Shall/Should]* produce both visual and audible alerts to the dispatcher when a timer is triggered.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

[13] Centers for Disease Control and Prevention (CDC): *Documentation for Immediately Dangerous To Life or Health Concentrations (IDHLs)* – http://www.cdc.gov/niosh/idlh/idlhintr.html.

6 SUPPLEMENTAL RESOURCE REQUEST AND TRACKING

Supplemental resource request and tracking refers to the ability for PSAP personnel to assign external resources, such as a towing company, to an incident whether it is via a vehicle owner's request for a specific towing company or a towing rotation list. In addition to tow companies, rotational lists have also been used for: utility companies, funeral homes, animal control companies, and persons willing to pick up fresh deer kills (hit by vehicles).

Operational Examples

- Law enforcement is on the scene of a vehicle crash and requests a tow truck off the rotation list. The dispatcher, using the CAD system's towing company rotation list, calls the next appropriate company. The system places that company at the "bottom" of the list in preparation for the next towing company request.
- Many jurisdictions handle tow companies via a rotational list to ensure fairness regarding opportunities. Often the rotational list is also broken down by zones, particularly if some companies only operate in certain zones.
- There is a winter storm occurring and call takers are getting numerous calls for trees down, blocking or partially blocking the road. The dispatcher and/or call taker keeps the highway department apprised of current tree-down locations and clears out the ones the highway department advises they removed.

6.1 Request Supplemental Resource



The CAD system has the ability to track external non-public safety agency resources; for example, in cases where a vehicle is being impounded or disabled such that it should be towed, the dispatcher needs the ability to request the services of a towing company. This request may be made by company name (vehicle owner-requested) or based on a rotational system within the system that is agency configurable. In cases where the owner does not have a preferred company, the system will recommend a company from the towing rotation file. A towing rotation prevents any one company from being favored over another. If resources other than those recommended by the rotation are selected, then the system should provide a field in which the dispatcher can document the reason for the exception. Other examples of supplemental resource tracking include utility companies, repair vehicles, animal control, Red Cross relief units, etc.

Sample Requirements

In order to support the *Request Supplemental Resource* function, the CAD system:

- *[Shall/Should]* be able to store, and easily retrieve, a file for standardized and *ad hoc* supplemental resources that may be recalled and requested as needed for services not available from the public safety agencies.
- *[Shall/Should]* make request and "dispatch" of said resources on the basis of the unique type of service needed, the geographic proximity to the site of the needed service, or a rotation of the unique service providers of a given type—or, a combination of methods.
- *[Shall/Should]* be able to create a unique or supplemental unit designation in real time.

- *[Shall/Should]* be able to record the activities of unique or supplemental units in the same manner in which agency response units are tracked and their activities recorded.
- *[Shall/Should]* allow for agency-configurable non-agency units to be recommended, such as the closest towing company recommendation when a unit is dispatched to an accident event type. The recommendation will take into account the rotation of towing companies.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

6.2 Request Supplemental Resource Rotation List



If supplemental service is unavailable, then the agency will obtain the contact information from the CAD system in order to contact and request service from the next eligible service. The system may provide a list of one or more services. This could be based on geographical requirements or by rotation.

Sample Requirements

In order to support the *Request Supplemental Resource Rotation List* function, the CAD system:

- *[Shall/Should]* store, and provide for easy retrieval, a list of authorized providers of unique or supplemental supplies or services.
- *[Shall/Should]* provide multiple sources of contact for each authorized vendor.
- *[Shall/Should]* be able to display the list of authorized service providers based upon geographical proximity to the site of need, by rotation, or by agency preference based upon contractual agreement.
- *[Shall/Should]* record the transactions that occur with supplemental or unique resources.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

6.3 Notify Supplemental Resource Service



The CAD system provides the ability to contact the supplemental resource and provide dispatch information by the dispatcher about the incident to which it is requested to respond. The availability of the entity to provide its services will be recorded. A supplemental service that cannot be contacted or informs the agency of its inability to respond within a prescribed time is considered unavailable to provide the service. A supplemental resource should be selected from a list. If a resource is unavailable, or is unable to respond in a reasonable time frame, then the user should contact the next listed resource until one is found that is available.

Sample Requirements

In order to support the *Notify Supplemental Resource Service* function, the CAD system:

- *[Shall/Should]* provide the ability to contact the supplemental resource; and, *[Shall/Should]* provide dispatch information by the dispatcher about the incident to which the resource is requested to respond.
- *[Shall/Should]* provide the ability to record the availability of the entity to provide its services.
    - A supplemental service that cannot be contacted or informs the agency of its inability to respond within a prescribed time *[Shall/Should]* be considered unavailable to provide the service.
- *[Shall/Should]* provide the ability to select a supplemental resource.
- If a resource is unavailable, or unable to respond in a reasonable time frame, then the user *[Shall/Should]* contact the next listed resource until one is found that is available.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

6.4 Enter and Update Supplemental Service Record



A record of supplemental service request is established to reflect the instance of the selection from the service provider list. If selectable by rotation, then this triggers the rotation to the next resource in the rotation. The rotation occurs regardless of the resources ability to respond.

Sample Requirements

In order to support the *Enter and Update Supplemental Service Record* function, the CAD system:

- *[Shall/Should]* provide the ability to create a record of the supplemental service request.
- *[Shall/Should]* accommodate selection from the provided list either at random, by geographic proximity to the site of need, or by rotation.
- *[Shall/Should]* trigger the next provider in the rotation, when selected by rotation and upon creation of the record
- *[Shall/Should]* process the rotation regardless of the requested resource's ability to respond.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

7 INCIDENT DISPOSITION

Incident disposition addresses those CAD system activities related to the closing of an incident including: assigning case numbers, entering an incident disposition, and transferring the call data to one or more RMS.

Operational Examples

- An incident will be closed when the units at the scene have completed the assignment, have provided the dispatcher an event/unit disposition (if required by agency policy) via voice, MDC transaction, or other CAD accessible application. The CAD CFS event is updated with disposition information. Depending on the agency's procedure, the primary unit may close the CFS event with a disposition or status. The CFS event is updated by a transaction performed by the dispatcher and/or MDCs to record the unit status and close the incident if the data received indicates that all units have completed their assignment related to the incident and no resources remain assigned to the incident. The incident will be classified with a specific disposition, generally provided by the primary unit. Depending on agency policy, secondary units sometimes provide one or more dispositions related to their involvement. Some agencies do not require any unit to provide a disposition and the event is closed when the last unit has been cleared from the event.
- When an incident is closed, information collected during by the CFS event may be automatically transferred from the CAD system to the RMS. Any updates made by the CAD operators on reopened events may be automatically transferred to the RMS, subject to agency policies.
- In instances where a duplicate CFS event has been created and is identified, one CFS event is disposed of (closed) and is cross-reference to the original CFS event. The CFS events will be linked for future retrieval purposes.

7.1 Determine Incident / Event Status



The incident will remain open and monitored. The status of the event may change as the situation is resolved. The system should provide the opportunity to change event status to the CFS event record as the situation evolves or a resolution is achieved. The optional MDC interface should allow the field user to enter a CFS event disposition that will update the CFS event in CAD and make that data available to the RMS.

Sample Requirements

In order to support the *Determine Incident / Event Status* function, the CAD system:

- *[Shall/Should]* provide the ability to change the event status as the situation evolves or a resolution is achieved.

The MDC interface:

- *[Shall/Should]* allow the field user to enter one or more event dispositions.
- *[Shall/Should]* allow the field user to update the CFS event in CAD and make that data available to the RMS.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

7.2 Utilize Incident Management



If an incident is in progress, then the CFS event is managed by continually updating the CFS event with any additional information reported by callers, other dispatchers or field units on scene. The resource recommendations may be revised based on additional information and may be added to or reassigned. The CAD system has the ability to dynamically update the CFS event with notations, updates, status changes, notifications, and make that data available for transfer to an RMS.

Sample Requirements

In order to support the *Utilize Incident Management* function, the CAD system:

- *[Shall/Should]* have the ability to dynamically update the CFS event with notations, updates, status changes, and notifications.
- *[Shall/Should]* make the updated CFS data available for transfer to an RMS.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

7.3 Determine Report Functionality



There are frequent needs to report CFS or summary CAD data outside of the CAD system, though specific requirements such as the data elements and timeliness may vary. Some examples are the National Incident-Based Report System (NIBRS), NFIRS, the National EMS Information System (NEMSIS) report, Uniformed Crime Report (UCR), or an electronic patient care report application. Guidelines are defined by agency policy, and are based upon a combination of incident type and incident disposition. The system should provide the ability to automatically transfer relevant CFS event data to an external reporting system. The system should also be able to determine, based upon incident type and/or disposition, whether an agency report is required.

If the incident is reportable, then the assignment of an incident number from the RMS may occur when the incident number is sent back with CFS event data to the RMS from the CAD system. CAD systems may accommodate either a push or pull of incident data from/to the RMS.

Sample Requirements

In order to support the *Determine Report Functionality* function, the CAD system:

- *[Shall/Should]* provide the ability to automatically transfer incident/event data relevant to external RMS or reporting systems.
- *[Shall/Should]* be able to determine, based upon incident type and/or disposition, whether an agency report is required.

- *[Shall/Should]* accommodate either a push or pull of incident/event data from/to the RMS.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

7.4 Record Disposition



The system should provide for the CFS event to contain the disposition of the incident. This may include a narrative in addition to the disposition type.

Sample Requirements

In order to support the *Record Disposition* function, the CAD system:

- *[Shall/Should]* provide for the CFS event to contain the disposition of the incident.
- *[Shall/Should]* provide for narrative to be added giving detail to the disposition.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

7.5 Send Data to Records Management System



Incident history (*i.e.* complete details on closed incidents) is typically maintained in a CAD system for a period of time based on operational requirements and/or state record retention rules. The CFS event is maintained in the CAD system to provide access to that database on a series of retrieval keys and/or parameters, (*e.g.* incident/event number, location, or date/time range). Incident history applies to the complete incident (*e.g.* CFS events, initial incident information, unit assignments, status changes, imbedded inquiries and responses, triage requests and results, comments, cross-references). Everything that was recorded during the taking and handling of the incident is available to the appropriate RMS integrated or interfaced with the CAD system, depending upon their design and configuration.

Depending on operational requirements, long-term storage of CFS event history records may be relegated to an RMS or a stand-alone incident system. If so, then the incident history system is used for data look-up and information retrieval, and it may also support extended statistical analysis processes based on types of events, response times, incidents by area, date/time, and so on. Because of the need for statistical analysis, incident history data needs to be structured to facilitate identifying specific types of data. This data should be made available to the appropriate RMS.

Sample Requirements

In order to support the *Send Data to Records Management System* function, the CAD system:

- *[Shall/Should]* provide the ability to exchange all CFS event information with an RMS.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

7.6 Assign Agency-Specific Report Numbers



If a report is required, then the CAD system will assign an *agency-specific report* (*i.e. case*) *number*, in addition to the CAD CFS event number, before the CFS event data is transferred to the RMS. This may happen at any time prior to sending the report, but will most likely be sent after the determination. The report number may be assigned from a table of incident numbers maintained in the CAD system in coordination with the RMS. Some RMS use the CAD-assigned event/system number as the report incident/case number. Department policies in this area are supported by the CAD system.

Sample Requirements

In order to support the *Assign Agency-Specific Report Numbers* function, the CAD system:

- *[Shall/Should]* assign an agency-specific report (*i.e.* case) number—if a report is required, and if required by agency policy—in addition to the CAD incident/event number, before the CFS event data is transferred to the RMS.
- *[Shall/Should]* allow for both the CAD CFS Event Number and the Agency Report Numbers to be fully configurable (*e.g.* "1 to n," "mmddyyxxxx," "mmddyyhhmmssxxx," "FY12xxxxxx," "2012-mmdd-xxxxx").

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

8 BUSINESS FUNCTION: CAD SYSTEM ADMINISTRATION

System administration is a core function of a CAD system. The various administrative functions and capabilities described below are required to keep the CAD system current and operational. Some of these administrative functions and capabilities should be completed on a daily or weekly basis; others are completed according to a predefined schedule; while others are only completed on an as needed basis. Since these CAD administrative functions and capabilities are frequently used by non-technical personnel, they should be implemented in the CAD system with an ergonomically structured GUI[14] so they can be easily accomplished.

Operational Examples

- Install and monitor the operating system (OS) for CAD Servers
- Install server OS upgrades and reinstall OS in event of server failure
- Review system logs and security logs
- Maintain server scripts
- Test disaster recovery
- Develop, maintain and provide workstations and MDCs with approved system images
- Ensure appropriate security and user permissions by agency and sub-group are identified and applied to the CAD system environment
- Perform patch management and service patch updates
- Conduct OS patch and service pack testing and deployment for servers
- Test, install and upgrade CAD antivirus releases and patches
- Develop, maintain and document CAD software configuration files
- Test and certify changes to baseline CAD configurations
- Authorize codes change migration to production via change management process
- Notify end users and migrate CAD updates to production environment
- Reference interface details workbook
- Monitor operational state of CAD Interfaces
- Manage and maintain CAD databases to include upgrades and patches
- Manage and maintain CAD databases and scripts
- Provide data for the CAD system ensuring currency, accuracy, integrity, and consistency
- Develop business rules for each data element or class of data provided for use in the CAD system

[14] A *GUI* refers to a modern, program/application interface that takes advantage of the computer's graphics capabilities to make the program easier to use. Well-designed GUIs free the user from learning complex command languages. A true GUI includes standard formats for representing text and graphics. Because the formats are well-defined, different programs that run under a common GUI can share data through cut and paste and other simple operations. Microsoft Windows is an example of a standards-based GUI.

- Act as custodian for all data assets provided for use in the CAD system
- Provide end user assistance for password reset requests
- Set application permissions settings
- Application-specific account activation/modification (*i.e.* capture account request, collect end user and authorization information)
- Application-specific account activation/modification (*i.e.* gain approvals per city/county/state processes; implement account changes; update audit information)
- Re-install applications on failed systems
- Perform routine server maintenance tasks
- Monitor server capacity, performance and reliability
- Ensure proper backups of system volumes

Whenever a new street is built or a response area changes within the geographic area for which a CAD system is deployed, the geofile used by the system should be updated to reflect the changes.

Confidential information is often processed and disseminated by the CAD system, and the system's security parameters should be continuously monitored and updated to ensure confidential data is properly handled and stored. In order to meet legal obligations and to support post incident analysis, all transactions performed by the CAD system and its users should be logged in a secure, confidential manner.

The CAD system's configuration parameters should be routinely updated to reflect changing dispatch policies, added or modified emergency units/apparatus and personnel, and other changes that occur in the dispatch environment.

Many of a CAD system's functions, such as the available incident types, field resource and apparatus statuses, are controlled by data stored in the CAD system's tables. Technically, these are describing database administration functions and, depending on the size of the jurisdiction, can be a separate responsibility from the *system* administrator. Techniques and procedures should be available in the CAD system to update these tables to keep them current with changing policies, operational procedures, resources and units/apparatus, and other changes in the system's environment.

Procedures, equipment and facilities are available to support emergency call receipt and dispatch in case the dispatch center should be evacuated and dispatch operations relocated to a different facility. There can be many reasons to relocate the PSAP, including a hazardous chemical spill in the vicinity of the dispatch center, noxious chemical release in the dispatch facility, or the complete loss of power or communications at the dispatch center. If the CAD system should be taken off-line or becomes inoperable due to an unforeseen situation, then a facility should be available within CAD once it becomes operational again to enter incident, resource deployment, and responder actions that occurred while the CAD system was down.

8.1 Geofile Maintenance



The CAD system's geofile is used for a variety of CAD functions including:

- Validating and standardizing location and address information.
- Assigning response agencies to an incident's location.
- Determining what resources should be assigned to an incident.
- Assigning (automatically) geographic boundaries (*e.g.* agency of jurisdiction, law enforcement zones/beats, fire response zones, sectors, neighborhoods, communities, precincts) to an incident's location.
- Calculating (automatically) the shortest and/or fastest driving route to an incident, and providing driving instructions to responding units.
- Displaying computerized maps containing relevant dispatch information.
- Determining the nearest confirmable address in the vicinity of a wireless emergency call.
- Identifying neighboring addresses as containing information of interest to event responders.

The CAD system's geofile should be updated to reflect changing conditions in the field. Typical changes that require a geofile update include:

- New street constructions
- Response agency boundary realignments
- New site/structure construction
- New and changing Landmarks (*e.g.* new parks, new names)
- Changes in descriptive (attribute) information stored in the geofile, including changes in attributes [*e.g.* street and landmark names, boundary IDs, address ranges of road center line (RCL) segments]

The CAD system's geofile can be maintained in three ways:

1) Using direct tools available within the CAD system (given the appropriate user permissions);
2) Uploading and/or converting a GIS-maintained set of geospatial datasets into the CAD system's internal geofile; and,
3) Uploading and/or converting (under NG9-1-1) the i3-compatible geospatial dataset from the appropriate Spatial Information Function (SIF).

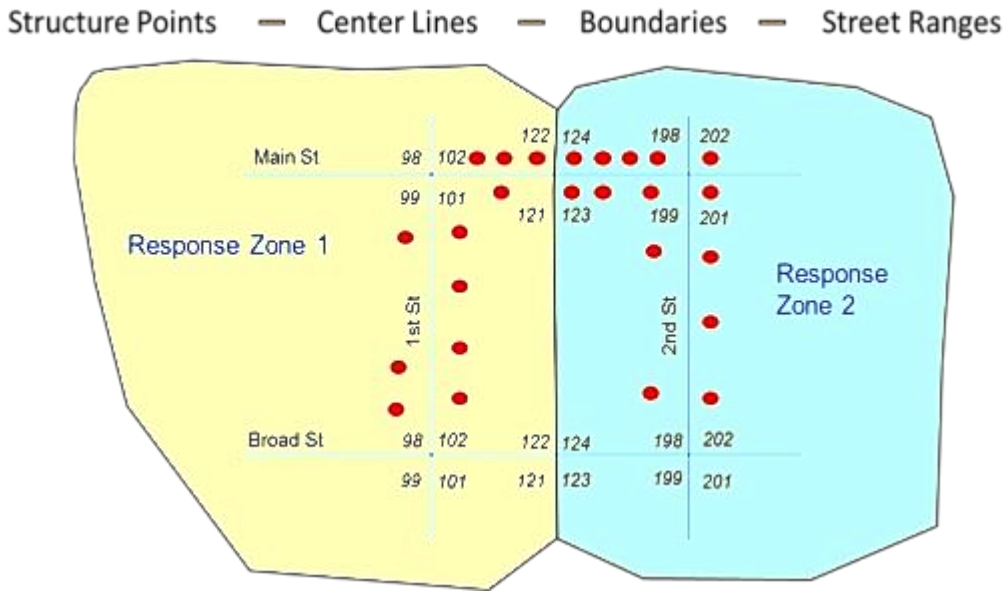
> Since the geofile is the basis for many CAD system decisions and functions, it is critical that the geofile is continuously monitored and updated on a timely basis.

NG9-1-1 emergency call routing, response agency assignment, call transfers, and other functions are performed through the use of GIS information. In order to avoid confusion and to minimize errors, the CAD system and the NG9-1-1 system should be using the same source of GIS data.

Typical Geofile

The typical CAD geofile contains *points* (*addresses*), *lines* (*RCLs*) and *polygons* (*relevant boundaries*), as well as metadata comprised of attribute information, including address ranges for each street segment and structure/site locations with their associated addresses.

FIGURE 3. TYPICAL CAD GEOFILE



Sample Requirements

In order to support the *Geofile Maintenance* function, the CAD system:

- *[Shall/Should]* validate all locations entered into or processed by the CAD system against the CAD system's geofile.
- *[Shall/Should]* provide an interactive, GUI-based address matching tool for assisting users to determine the location of incidents that do not have an exact geofile match for their initially-entered location.
- *[Shall/Should]* be capable of determining X,Y coordinate values that represent the location of incidents whose locations have been validated.
- *[Shall/Should]* be capable of displaying coordinates anywhere on the map with mouse over.
- *[Shall/Should]* support coordinate-based operations including X,Y, Lat/Lon, and USNG.
- *[Shall/Should]* make possible integration of the CAD system's geofile with Global Positioning Satellite (GPS), AVL, and Automatic Person Location (APL) systems.
- *[Shall/Should]* support X,Y coordinate-based geographic searches for such things as nearby hazardous materials, duplicate incidents, and premises information at or near an incident's location.
- *[Shall/Should]* be capable of importing geographic boundary information (*e.g.* station boundaries, jurisdictional boundaries, reporting districts, response zones, neighborhoods, precincts) from GIS and other geographic data sources.
- *[Shall/Should]* be capable of importing topologically-structured street networks and other linear features (*e.g.* rivers, streams, utility right of ways, bus routes) from GIS and other geographic data sources.

- *[Shall/Should]* be capable of importing point data (*e.g.* landmarks, parcel address points, business locations, retail store address points, fire hydrants) from GIS and other geographic data sources.
- *[Shall/Should]* be capable of importing other types of geographic data (*e.g.* park boundaries, rectified aerial photography, trailer parks, apartment complexes) from GIS and other geographic data sources.
- *[Shall/Should]* include location databases such as hazards, general premises information, street closures, and other user-definable GIS type data.
- *[Shall/Should]* support parcel-level GIS information and use this information for address/location validation.
- *[Shall/Should]* support multiple layers of information; for example, the storage of building footprints, aerial photographs and other images (*i.e.* pictures of specific buildings) that are associated with specific areas and addresses.
- *[Shall/Should]* maintain the CAD system's geofile while the system is live and operational.
- *[Shall/Should]* support boundary assignments (*i.e.* determining the response zone and jurisdiction for each incident) in real time by processing the incident's X,Y coordinates against the RCL and/or address point file, and the appropriate boundary files.
- *[Shall/Should]* support duplicate incident checks based upon the location of the incident.
- All incidents located within the CAD system's duplicate incident search radius *[Shall/Should]* be checked as potential duplicates.
- *[Shall/Should]* should meet i3 standards and functions in order to comply with NG9-1-1 requirements.
- *[Shall/Should]* include interactive tools for validating the accuracy and completeness of the geofile.
- *[Shall/Should]* be able to support different search distance criteria for different types of incident situations and hazards (*e.g.* a search radius of 300 feet will be used for hazardous conditions, and a search radius of 1,320 feet will be used to identify potentially duplicate incidents).
    - CAD system administrators *[Shall/Should]* be able to modify these search distance parameters.
    - CAD users *[Shall/Should]* have the ability to select the unit of measurement necessary (feet versus meters).
- *[Shall/Should]* generate an audible and/or visual alert when any potential duplicate incidents are identified.
- *[Shall/Should]* include the capability for manually editing and entering any geographic data required by, or imported into, the system's GIS (given the appropriate user permissions).

Relevant Technical Standards / Guidelines

- *NENA 08-003 Functional and Interface Standards for the NENA i3 Solution* – http://www.nena.org/?page=Standards

8.2 Security



Sufficient security should be available within the CAD system to prevent unauthorized access to system modules and data. Confidential, tactical and life critical information and functions are stored and available within most CAD systems. This information and functions should only be accessed by authorized individuals.

CAD system security typically involves establishing a set of roles (*i.e.* security groups) within the system and enabling a set of system access privileges for each role. System users are assigned to a role, which then establishes their credentials and permissions within the system. Alternately, each user may individually be assigned CAD system access privileges.

Since Criminal Justice Information Services (CJIS) data may be accessed by CAD system operators, the CAD system should meet CJIS security requirements. CJIS security policies will soon require two-factor authentication (*e.g.* user ID and password plus biometric identifications), which means that most CAD systems will eventually be required to use two-factor authentication prior to enabling CAD operators to use the system.

Sample Requirements

In order to support the *Security* function, the CAD system:

- *[Shall/Should]* employ data security measures that are compliant with applicable state and federal security standards.
- *[Shall/Should]* employ data encryption that meets CJIS security policy standards for any exchange or transmittal of CAD data between remote devices and CAD system servers.
- *[Shall/Should]* provide appropriate safeguards to ensure that only authorized devices and users are allowed access to the CAD system and stored information.
- *[Shall/Should]* provide a security profile to control individual user access to the various modules, applications, functions, features, and data available within the CAD system.
- *[Shall/Should]* provide security to ensure that fire and EMS personnel do not have access to law incidents when CJIS data is restricted to only law enforcement user access.
- *[Shall/Should]* meet CJIS Security Policy requirements.
- *[Shall/Should]* validate each user's credentials through a mandatory logon process before being granted access to any functions or data available within the CAD system.
- *[Shall/Should]* enable a user replacing an existing user to quickly log off the existing user and logon without the need to exit from CAD or re-start the CAD application (*i.e.* when two-factor authentication does not apply.)
- *[Shall/Should]* enable system administrators to create and maintain a centralized and indexed database containing information about each system user, including their unique user ID, password, contact information, and security profile.
- *[Shall/Should]* enable system administrators to define individual user access privileges and assign them to security groups.
- *[Shall/Should]* provide a method for authorized users to reset a user's password.

- *[Shall/Should]* associate the user ID and workstation ID with all CAD system transactions, including data entry and report generation.
- *[Shall/Should]* limit access to the centralized user security database to only specifically authorized users.
- *[Shall/Should]* establish security profiles that are assigned to individual users or user groups based on personnel classifications (*e.g.* call taker, dispatcher, system administrator, supervisor).
- *[Shall/Should]* prohibit deletion of any data entered into a CFS event.
- *[Shall/Should]* provide application and module level security that enables certain users to access specific CAD system functions and application modules, while keeping other users from accessing these same functions and modules.
- *[Shall/Should]* provide data entry form security that enables certain users to access specific data entry forms, while keeping other users from accessing these same data entry forms.
- *[Shall/Should]* provide record type security that enables certain users to access specific CAD system record types, while keeping other users from accessing these same record types.
- *[Shall/Should]* provide transaction level security that enables certain users to access specific transaction types (*e.g.* criminal history queries to NCIC), while keeping other users from accessing these same transaction types.
- *[Shall/Should]* provide data field level security that enables certain users to access specific CAD data fields, while keeping other users from accessing these same data fields.
- *[Shall/Should]* facilitate the use of unique user IDs and passwords to control CAD system access and privileges.
- *[Shall/Should]* be capable of using biometric identification (*e.g.* thumb print identification, retinal ID) to control system access and privileges.
- *[Shall/Should]* provide a "single entry" to enable logons to multiple authorized systems that are available through the system (*e.g.* NCIC, Nlets).
- *[Shall/Should]* limit access to system functions and data by physical device (*e.g.* PCs, terminals), as well as by user ID.
- *[Shall/Should]* have the capability to automatically log-off CAD workstations based on inactivity periods set by the system administrator for specific user groups, users and workstations.
- *[Shall/Should]* provide the ability to "lock out" a user after a system administrator defined number of failed attempted logons.
- *[Shall/Should]* require users to change their individual password after a system administrator configurable time limit for use of the same password expires or a set time period (*e.g.* 90 days).
- *[Shall/Should]* provide the ability for individual system users to change their passwords.
- *[Shall/Should]* provide the capability for individual user name change (*e.g.* getting married) and *[shall/should]* keep a link to historical data.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

8.3 Logging



In order to be able to meet post-incident analysis and legal requirements, ***all*** CAD transactions should be logged in the system's transaction audit database, including transactions dealing with:

- Incidents
- Resource statuses, locations, and usage
- System administrative functions
- Geofile updates and changes
- System alerts and notices and users actions related to the alerts and notices
- User actions, including printing, viewing, editing, and deleting existing or entering new information into the system
- Queries
- Reports
- Security violations and attempted breeches
- System error messages and users actions related to the error messages

Access to the CAD system's transaction audit database should be limited to users that are specifically authorized to view transaction audit information. The transaction audit database should be searchable by authorized users.

Sample Requirements

In order to support the *Logging* function, the CAD system:

- *[Shall/Should]* include a transaction audit database that contains all system transactions and that includes the logon identification (*i.e.* user ID and workstation ID), date and time stamp, transaction type, contents before ID, and contents after the transaction completes.
- *[Shall/Should]* enable system administrators to turn the transaction audit log function on and off by application module, transaction type, specific data entry form(s), specific tables and data fields within tables, individual users, user groups, and various combinations of these factors.
- *[Shall/Should]* enable authorized system users to search the transaction audit database by date and time ranges, by application module, transaction type, specific tables and data fields within tables, specific data entry forms, individual users, user groups, workstation ID, and by various combinations of these factors.
- *[Shall/Should]* enable authorized system users to create formatted reports and/or export the results of transaction audit database queries and searches.
- *[Shall/Should]* enable authorized system users to generate statistical reports on transactions contained in the transaction audit database for all users, a subset of users and/or user groups, for a specified date and time range, and for various combinations of these factors.
- *[Shall/Should]* prohibit any changes to the contents of the CAD transaction audit database.

The CAD system's CAD transaction audit database:

- *[Shall/Should]* store all transactions completed on open/active incidents, including the transaction's date and time stamp, the user and workstation ID performing the transaction, and the before and after results of the transaction.

- *[Shall/Should]* store all system messages, including the message's date and time stamp, the user and workstation ID sending and receiving the message, and the message contents.
- *[Shall/Should]* store transaction information associated with all CAD configuration parameters and files, including any time a user views, prints, edits, ads, or deletes the configuration parameters and/or CAD system configuration file records.
- *[Shall/Should]* should capture the messages and associated information (*e.g.* date and time stamp, user ID, workstations ID) of user and system generated queries to interfaced system and databases (*e.g.* NCIC, Nlets).
- *[Shall/Should]* should capture the date, time and user ID associated with previous incident history access.
- *[Shall/Should]* should capture transaction information associated with all CAD security transactions, including any time a CAD user views, prints, edits, ads, or deletes the security information within the CAD system.
- *[Shall/Should]* store transaction information associated with all CAD system modifications completed by system administrators, including administrator user ID, date/time of modification, modification made, and table value prior to the completed modification.
- *[Shall/Should]* store the date, time, workstation ID, and user ID associated with unsuccessful sign-on attempts.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

8.4 Configuration



The CAD system contains configuration parameters that enable it to be tailored to meet the requirements of the agencies using it rather than having to be customized to meet those requirements. The CAD configuration parameters used to tailor the system are only accessible by specifically authorized CAD system administrators. CAD configuration options are flexible and cover most, if not all, of the various items that can be tailored in the CAD system including:

- Establishing the types of agencies and their unique parameters (*e.g.* fire, law enforcement, EMS, fire and EMS) that will be included in the system.
- Entering and modifying the various types of resources that will be used or dispatched by the system.
- Defining the statuses that can be assigned to resources that will be used or dispatched by the system.
- Turning timers on and off and setting their timing parameters (*e.g.* configuring a timer that monitors how long incidents remain in the pending incident queue without being assigned any resources and causes CAD to notify a supervisor or raise the priority of incidents if the timer is exceeded; configuring officer safety check timers).
- Establishing the type of incidents, priorities, and disposition codes that will be available in the system.

- Establishing dispatch policies for each incident type and agency in the system.
- Setting up the formats of agency case report numbers issued by the CAD system.
- Establishing mutual and automatic aid agreements and their impacts on dispatch policies.
- Establishing deployment and response plans.
- Configuring default report formats and contents.
- Configuring system alerts and their formats.
- Establishing and modifying keyboard function actions.
- Establishing workflow parameters.
- Establishing workstation and user preferences (*e.g.* color, font, window locations, display sort orders, tab orders).

CAD configuration parameters need to be routinely updated or modified to keep abreast of evolving technology and operating procedures. GUI-based tools should be available to authorized system administrators to easily update the CAD system's configuration parameters. It should not require taking the CAD system offline in order to change or activate changes in CAD configuration parameters.

Sample Requirements

In order to support the *Configuration* function, the CAD system:

- *[Shall/Should]* enable authorized system administrators to configure the CAD system to meet the requirements of the agencies using the system by creating and modifying CAD configuration parameters.
- *[Shall/Should]* enable authorized system administrators to modify CAD configuration parameters without the requirement for programmer or other support from the manufacturer of the CAD system.

CAD configuration parameters:

- *[Shall/Should]* include functionality for table driven and directly modifiable functionality by authorized system administrators.
- *[Shall/Should]* include functionality for interactive, menu-driven, GUI-based tool that allows authorized administrators to easily update and modify parameters.
- *[Shall/Should]* include functionality for on-line help that lists all of the available options for a configuration parameter, and a description of the impacts resulting from changing the parameter to each of its available options.
- *[Shall/Should]* include functionality for modifications to CAD configuration parameters when the CAD system is active without having to shut the entire CAD system down or restart it.
- *[Shall/Should]* include functionality for modifying agency and user specific workflows, such as when and under what circumstances a CFS event is automatically routed from a call taker to a dispatcher and which users (*e.g.* call takers, dispatchers, supervisors) receive system routed CFS events.
- *[Shall/Should]* include functionality for specifying the agencies that will be included in the CAD system, along with their attributes (*i.e.* fire department, volunteers, law enforcement agency).

- *[Shall/Should]* include functionality for specifying and modifying the type of resources available in the system.
- *[Shall/Should]* include functionality for specifying the incident types that will be processed by the system.
- *[Shall/Should]* include functionality for entering and modifying dispatch policies that specify the type of resources that are dispatched to specific incident types.
- *[Shall/Should]* include functionality for configuring different system dispatch policies for each incident type, priority and agency using the system.
- *[Shall/Should]* include functionality for specifying the type of alerts and timers available in the system and their specific attributes (*e.g.* on/off, time interval, triggers, display features).
- *[Shall/Should]* include functionality for entering and modifying the type of dispositions, priorities, and other CFS event related parameters of the CAD system.
- *[Shall/Should]* include functionality for specifying the starting point and formats of case numbers created by the CAD system for each agency using the system.
- *[Shall/Should]* include functionality for specifying the sort order, layout, color, font, and other appearance and operational attributes of the CAD system's windows and menus.
- *[Shall/Should]* include functionality for modifying the look and feel of CAD workstations.
- *[Shall/Should]* include functionality for modifying the look and feel of the tactical map display available in the system (*e.g.* setting up the graphic information appearing at different zoom levels, predefined zoom levels for different incident types, icons).
- *[Shall/Should]* include functionality for modifying the display and functional characteristics of CAD system queues (*e.g.* pending incident queue, incident queue, active incident queue, stacked incidents queue).
- *[Shall/Should]* include functionality for modifying the display and functional characteristics of the CAD system's resource recommendations.
- *[Shall/Should]* include functionality for modifying the display and functional characteristics of interfaced systems and gateways (*e.g.* 9-1-1 call interfaces, paging and other responder alerting interfaces, NCIC and other criminal database interfaces, mobile computer system).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

8.5 Table Maintenance



The flexibility needed in a CAD system requires that the data used to support all CAD functions and operations be maintained in tables that can be changed by the agency. Each department will have its own set of procedures that should be followed with regard to table maintenance.

In addition, the CAD system should be flexible enough to allow the system setup to reflect the procedures at the time the system is initially installed, and to be changed when such procedures change.

Procedures for performing CAD table maintenance are typically defined and maintained in a separate document or they may be available for reference online as a CAD help file.

> Requirements for CAD geofile maintenance are found in 'Section 8.1 Geofile Maintenance' and are, therefore, are not addressed here.

Sample Requirements

In order to support the *Table Maintenance* function, the CAD system:

- *[Shall/Should]* include CAD tables that are maintained using entry windows.
- *[Shall/Should]* include CAD table maintenance entry windows that have context-sensitive, field-level help.
- *[Shall/Should]* enable changes made to CAD tables to become immediately effective and *[shall/should]* not affect overall CAD system availability nor require any CAD system down time.

  > This does not preclude the refresh of individual workstations or other CAD devices as required by the CAD manufacturer.

- *[Shall/Should]* allow agencies to define additional data elements based on their operational requirements.
- *[Shall/Should]* provide the ability for tables to be defined to support the maintenance of the following CAD objects, including, but not limited to:
  - Agencies
  - BOLOs, including location, person, and vehicle
  - Clearance/disposition codes
  - Hazards
  - Hydrants
  - Incident/event types
  - Fire Stations
  - Memos
  - Messages (*e.g.* canned, scheduled)
  - Notifications
  - Personnel
  - Rosters
  - Run cards/response plans
  - Service types (*i.e.* law enforcement, fire, EMS)
  - Skills (personnel)
  - SOPs
  - Units
  - Unit attributes (*e.g.* ALS, BLS, Hurst tool)
  - Unit statuses (*i.e.* dispatched, en route, arrived, cleared)
  - Unit Types (*e.g. i.e.* patrol car, motorcycle, engine, ladder, pumper)
  - Vehicles

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

8.6 Communication Center / PSAP Relocation



Relocation could be the result of a major incident rendering the existing location unusable, or relocation involving a new location during a remodel of the existing location. The support of an incident that requires that the dispatch center be moved to an off-site secure location should include a hardware system and network connectivity that will support the creation of an off-site, real-time backup server at the relocated communications center. Items that should be considered include: 9-1-1 lines, law enforcement and fire/EMS business lines, fire alarm circuits, logging/recording of phones and radio, dispatcher radio consoles, computer aided dispatch consoles, network, uninterrupted power system (UPS), mapping, and other systems. Relocation of all these items should occur while providing uninterrupted coverage.

Sample Requirements

In order to support the *Communication Center / PSAP Relocation* function, the CAD system:

- *[Shall/Should]* meet PSAP industry best practices and CJIS requirements.
- *[Shall/Should]* account for replacement or the movement of any necessary existing equipment including base computers, terminals, network, and personnel.
- *[Shall/Should]* account for a data-backup plan.
- *[Shall/Should]* account for coordination of external inputs to the CAD system from third-party vendors (*e.g.* telephone, data, 9-1-1) for a minimal loss of functionality.
- *[Shall/Should]* provide for access to a copy of the production system through the backup or disaster recovery environments.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

8.7 CAD Catch-Up



CAD catch-up is the ability to recover missed information due to the interruption of CAD services, allowing the agency to enter activity data performed during the interruption of service; for example, a hardware failure of the CAD system causes the entire system to be inoperable for a few hours, and written dispatch call-taking is established. Once the system is restored, all CAD information would be manually entered and times updated for correct reporting. Since the times captured during the CFS event creation would be several hours after the event, the entering individual can manually update the CFS event times.

Sample Requirements

In order to support the *CAD Catch-Up* function, the CAD system:

- *[Shall/Should]* have the ability to manually open and create a CFS event sheet.
- *[Shall/Should]* provide the ability to log the entering individual's information and time of entry.

- *[Shall/Should]* provide the ability for all information to be entered without any restrictions, and times/dates changed to reflect the actual time that notice of the CFS event was received.
- *[Shall/Should]* denote the manually-entered CFS event so there is a record that the CFS event was not entered when it was actually received.
- *[Shall/Should]* provide ability to manually designate the "starting" incident number (*i.e.* the last incident +1 for the starting number once the system is restarted).
- *[Shall/Should]* allow for simultaneous automatic and manual entry without degradation.
- *[Shall/Should]* include all the information in back entered records that a live incident/event sheet should require.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9 SYSTEM FUNCTIONS

For the purposes of this document, *system functions* refer to internal functionality. Some of these are seamless to the end user, while some are routine. Regardless, they are all integral parts to a CAD system and provide critical functions and/or capabilities.

Operational Examples

- Law enforcement is responding to a domestic at a particular address. The CAD system alerts the operator and, possibly, the responding unit via MDC, of previous calls for service at that address, outstanding warrants for persons living at that address, and other hazards recorded at that address previously (*e.g.* vicious dogs, hazardous materials).
- Some CAD operators prefer using a command line, while others like the mouse – the CAD system handles both.
- The CAD system records items like time stamps and individual key strokes.

9.1 Notifications



Law enforcement, fire, and EMS functionality requires additional enhanced paging, text-based alerting, SMS, MMS, and other messaging. CAD systems have the ability to associate notifications with specific incident types and locations, by time of day and day of week, to individuals or groups; for example, a fire in a federal building may require notification to a staff chief, or a shooting may generate an automatic notification to the criminal investigations supervisor. Since some staff of organizations operate on rotating schedules, the person who receives the notification may be dependent upon the shift on duty at the time of the incident.

Definitions for notification triggers support a wide variety of parameters (*e.g.* incident location attributes, such as: fire jurisdiction, fire zone, fire district, fire battalion, fire first due area, law enforcement precinct, law enforcement beat, assigned unit, assigned unit jurisdiction, incident type, response type, incident category, incident status, alarm level, incident milestone/benchmark, incident jurisdiction shift on duty, assigned unit jurisdiction shift on duty).

Some CAD systems may be able, either internally or through an interface to a third-party application, to monitor EMS system loading and dispersal and trigger notifications when pre-configured thresholds are met.

Sample Requirements

In order to support the *Notifications* function, the CAD system:

- *[Shall/Should]* enable the system administrator to define the rules for automatic CFS event notifications.
- *[Shall/Should]* provide the ability to create messages that are retained in the system and sent at pre-specified times.
- *[Shall/Should]* provide the ability to maintain a log of all messages processed by the system.
- *[Shall/Should]* allow the user to send and store messages to other users, groups, positions, or mobile devices.

- *[Shall/Should]* allow a message to be sent to multiple recipients and/or groups.
- *[Shall/Should]* log all sent messages.
- *[Shall/Should]* provide the ability to create and maintain automatic reminders of scheduled activities (*e.g.* radio tests):
    - Daily
    - Weekly
    - Monthly
    - Annually
    - User-defined (*e.g.* 30 minutes, 15 minutes, first day of the month)
    - Multiple activities or reminders per time slot

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.2 Contact List



Dispatchers may be required to place outbound phone calls or pages to individuals or groups of individuals that are not assigned to a unit. The *contact list* function allows the creation, search and maintenance of such contacts and their contact information. In some cases, the contact list will be interfaced to the phone system to create a point-and-click capability for outbound calling. This would include call-back and overtime lists to cover vacancies and extreme emergencies.

Sample Requirements

In order to support the *Contact List* function, the CAD system:

- *[Shall/Should]* allow a message to be sent to multiple recipients and/or groups.
- *[Shall/Should]* be able to log all sent messages.
- *[Shall/Should]* provide an emergency contacts list, to include:
    - Contact name
    - Street address
    - City
    - State
    - Zip
    - Telephone numbers
    - Relationship
    - User-defined/configurable fields

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.3 Premises Information / Hazards



This capability allows for the CAD system to appropriately provide information specific to a particular location or premises. The alert

information can be manually entered, based on previous incidents, and/or provided by an interface to another RMS (*i.e.* law enforcement RMS). Examples of premises hazards information can include:

- Hazardous or flammable chemicals on site (*i.e.* type and quantity)
- Resident has outstanding warrant, history of violence
- Aggressive dogs on site
- Locations of special or critical equipment (*e.g.* fire alarm panels, automatic external defibrillators, and sprinkler shut off valves)
- Locations on the list of Critical Infrastructure/Key Resources (CI/KR)

This capability should also include temporary hazards, such as holes in floors, buildings under renovation, and restricted access situations. EMS premises information may also include patient history, such as medical conditions (*e.g.* on oxygen), combative patients, and patients requiring additional staffing resources because of size. An alternative solution is to provide the ability to attach other data sources (*e.g.* electronic documents, PDF, WAV, JPEG, and other files) to the CAD map. Premises information is not limited to specific addresses, as it may also be applicable to a geographic area.

Sample Requirements

In order to support the *Premises Information / Hazards* function, the CAD system:

- *[Shall/Should]* provide the ability to enter a premises location by address, cross street or latitude/longitude.
- *[Shall/Should]* provide the ability to capture, maintain or interface to specific premises information types for operators:
    - Hazardous materials
    - Hazardous conditions
    - Lock codes
    - Dangerous animals
    - Handicap
    - Emergency contact information
    - Unit safety
    - Warrants
    - Alarms
    - Protective Orders, Sexual Offenders
    - Fire Pre-plans
    - Other user-defined premises fields/information
    - Electronic attachments (*e.g.* images, files)
- *[Shall/Should]* provide the ability to automatically create (*i.e.* upon closing of an incident) premises history based on pre-determined criteria.
- *[Shall/Should]* provide the ability to define valid date ranges for time-limited premises information at a given location (*i.e.* information valid between start date and end date), and to notify supervisor of pending expiration dates.
- *[Shall/Should]* provide the ability for supervisors to delete premises information for a given address or location based on expiration date and/or time of record, with prompted review prior to deletion (*i.e.* minimum of five years, on-line storage).

- *[Shall/Should]* provide the ability to define criteria for automatic premises information purges and activate or deactivate this feature.
- *[Shall/Should]* provide the ability to verify that premises warning or hazard information has not been affected by changes to the geofile.
- *[Shall/Should]* provide the ability to view premises information for a specific suite/apartment/unit, or to view all premises information for an entire building.
- *[Shall/Should]* provide the ability to automatically embed premises information into the event history at the time the event is created.
- *[Shall/Should]* create a permanent record of the premises information in the event history.
- *[Shall/Should]* provide (or interface to) a "cautions" file to contain information pertaining to dangerous individuals possibly residing at that location or near proximity, and exceptional persons at the location, such as an emotionally disturbed person.
    - This *[Shall/Should]* include a caution type category and free form narrative.
    - The caution type *[Shall/Should]* be searchable.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.4 Communications Center / Public Safety Answering Point Standard Operating Procedures



The CAD system provides the ability to store and easily retrieve SOPs for the PSAP. Many responses to incidents require actions that are not unit-based responses, and, thus, may not be part of a designated response plans. Nonetheless, they are important items that need to be executed.

Depending on the agency, geographic area, incident type, and alarm level, the dispatcher may be required to complete specific tasks; a user may be asked to perform one task (*e.g.* place one phone call to a specific agency) or there may be multiple tasks (*e.g.* place two notification phone calls: one to a utility company and one to an agency). An SOP tool prompts the user to ask for additional information, perform certain tasks, or relay critical information to responding units or other responders. Retrieval of relevant SOPs should be accessible from the incident record, and should be associated with the location, incident type, unit, or special skilled personnel responding. This feature is similar to common help functionality.

Sample Requirements

In order to support the *Communications Center / Public Safety Answering Point Standard Operating Procedures* function, the CAD system:

- *[Shall/Should]* provide the ability to store and easily retrieve SOPs for the PSAP.
- *[Shall/Should]* provide a SOP tool to prompt the user to ask for additional information, perform certain tasks, or relay critical information to responding units or other responders.

- *[Shall/Should]* provide a method where the retrieval of relevant SOPs are accessible from the CFS event information window and associated with the location, incident type, unit, or special skilled personnel responding.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.5 Agency-Specific Incident / Location / Unit Standard Operating Procedures



The CAD system is able to store SOPs that are associated with incident types, locations and/or units. These SOPs are available for viewing and/or transmitting when an associated incident type is encountered, the response is to a specific location with unique response or operational requirements, and/or specialized units are assigned to the incident. Optionally, more sophisticated functionality may include alert and check off of tasks, notifications made, or other issues capable of being tracked.

Sample Requirements

In order to support the *Agency-Specific Incident / Location / Unit Standard Operating Procedures* function, the CAD system:

- *[Shall/Should]* be able to store SOPs that are associated with incident types, properties and/or units.
- *[Shall/Should]* make these SOPs available for viewing and/or transmitting when an associated incident type is encountered, the response is to a specific location with unique response/operational requirements, and/or specialized units are assigned to the incident.
- *[Shall/Should]* include (optional) more sophisticated functionality (*e.g.* alert and check off of tasks, notifications made, or other issues capable of being tracked).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.6 Remote Access



A CAD system supports remote access by users outside of the communications center. This access includes permission-based views of CAD system data by certain workstations and/or individuals. Remote access should include security-controlled, web-based access. The system is also capable of remote access from a separate location, such as a mobile command post or a secondary location.

Sample Requirements

In order to support the *Remote Access* function, the CAD system:

- *[Shall/Should]* support remote access by users outside of the communications center.

- *[Shall/Should]* provide access that includes permission-based views of CAD data by certain workstations and/or individuals.
- *[Shall/Should]* provide remote access that includes security-controlled, web-based access.
- *[Shall/Should]* be capable of remote access from a separate location, such as a mobile command post or a secondary location.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.7 CAD Workstation-to-CAD Workstation Messaging



CAD system functionality includes short messaging from one CAD workstation to another. The agency can disable this function if desired. This functionality includes the ability to create message groups, whether they are dispatch workstations, MDCs or other communications devices. This also includes the ability to create user definable "canned" messages for selection and distribution to other system users.

Sample Requirements

In order to support the *CAD Workstation-to-CAD Workstation Messaging* function, the CAD system:

- *[Shall/Should]* provide short messaging from one CAD workstation to another.
- *[Shall/Should]* include the ability to create message groups, whether they are dispatch workstations, mobile computers, groups within the PSAP, or other communications devices.
- *[Shall/Should]* enable the system administrator to disable this function if desired on an agency basis.
- *[Shall/Should]* log all messages.
- *[Shall/Should]* provide the ability to create user definable "canned" messages for selection and distribution to other system users.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.8 Incident Command Support



The CAD system supports the functions required by the NIMS and the ability to provide data to support NIMS-required reporting from an RMS. This includes the ability to track roles, tasks, and situation reports. This may either be provided directly in a CAD system or be integrated with an external system.

Sample Requirements

In order to support the *Incident Command Support* function, the CAD system:

- *[Shall/Should]* be able to support the functions of the NIMS and to provide data to support NIMS-required reporting from an RMS.
- *[Shall/Should]* provide the ability to track roles, tasks and situation reports.
- *[Shall/Should]* provide NIMS functions directly or through an interface with an external system.
- *[Shall/Should]* interface to [insert specific application/product here] incident command software.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.9 Narrative Field "Shorthand" / Auto Text



The CAD system provides the ability to recognize character patterns and automatically fill in expanded text; for example, a dispatcher enters 'PPE' in a comments field and the text expands to indicate that 'personal protective equipment' is required on an incident. The CAD system automatically expands the shorthand into a full description and saves it into the narrative.

Sample Requirements

In order to support the *Narrative Field "Shorthand" / Auto Text* function, the CAD system:

- *[Shall/Should]* provide the ability to recognize character patterns and automatically fill in expanded text.
- *[Shall/Should]* expand (automatically) the shorthand into a full description and save it into the narrative.
- *[Shall/Should]* allow the agency to add agency-specific shorthand terms and their expansions.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.10 Command Line / GUI



The CAD system includes the ability to be operated via a command line entry, mouse and keyboard, or both.

Sample Requirements

In order to support the *Command Line / GUI* function, the CAD system:

- *[Shall/Should]* include the ability to be operated via a command line entry, mouse and keyboard, or both.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.11 Date/Time Stamps



CAD activities, such as status changes, task accomplishments (*i.e.* Fire Attack Initiated, Time Fire Declared Under Control, Time at Patient, Time of Contact with *Medical Control*[15]), and notifications, as well as many other CAD system transactions, should be "time stamped" with the time they occur and be logged by the system into the CFS event. This is important for performance metrics, QA, training, documentation, and evidentiary purposes. Original time stamps are saved, even if they are overridden. Time stamp overrides are security protected and any changes are documented on the incident, including the ID of the person performing the modification and the reason for the modification.

Sample Requirements

In order to support the *Date / Time Stamps* Function, the CAD system:

- *[Shall/Should]* stamp date/time and log CAD activities, such as status changes, task accomplishments (*i.e.* Fire Attack Initiated, Time Fire Declared Under Control, Time at Patient), and notifications, as well as many other system transactions and the time they occur.
- *[Shall/Should]* save original time stamps even if they are overridden.
- *[Shall/Should]* protect time stamp overrides; and, any changes *[Shall/Should]* be documented on the incident, including the ID of the person performing the modification and the reason for the modification.
- *[Shall/Should]* maintain all time stamps to be minimally accurate to the second (*e.g.* hh:mm:ss).

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.12 Unit Status Transitions Matrix



Unit status transitions that do not conform to the business rules of the agency should not be permitted. If a unit has an 'En Route' status and is the only unit assigned to the incident, then it is not permissible to change the status of the unit (*e.g.* 'Available in Quarters,' 'Available on Radio', or 'Training') unless the CFS event has been reassigned to another unit, the unit is pre-empted from the call causing the CFS event to be re-submitted to the dispatch queue, or the CFS event has been cancelled. Any unit status transition must be fully recorded/documented in the CFS event for audit purposes.

Sample Requirements

In order to support the *Unit Status Transitions Matrix* function, the CAD system:

- *[Shall/Should]* prohibit unit status transitions that do not conform to the business rules of the agency.

[15] *Medical control* means advice and direction provided by a physician or under the direction of a physician to certified first responders, emergency medical technicians, or advanced emergency medical technicians who are providing medical care at the scene of an emergency or en route to a health care facility.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.13 Single Sign-on for CAD and CAD Sub-systems



A PSAP or secondary public safety communications center operates with multiple technology- and network-based platforms, each with their own credentialing and access rights functions. The CAD system is designed to provide a single sign-on for CAD and its integrated sub-systems. The agency reserves the right to determine what systems, if any, can be accessed via single sign-on.

Sample Requirements

In order to support the *Single Sign-on for CAD and CAD Sub-systems* function, the CAD system:

- *[Shall/Should]* be designed to provide a single sign-on for CAD and its integrated sub-systems.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

9.14 Multi-Agency / Multi-Jurisdictional Capability



The CAD system provides the capability to seamlessly create multiple independent and linked incidents for each agency or jurisdiction associated to the incident without duplicating any data-entry.

The CAD system can determine the need to automatically generate multiple CFS events related to a single incident, or to transmit CAD data to external systems based on various pre-designated factors, including: CAD incident type, incident location, incident resource recommendations, or combinations of these factors.

The CAD system can support the creation of events for other agencies or jurisdictions based on dispatcher or MDC-equipped unit actions to request such services.

Sample Requirements

In order to support the *Multi-Agency / Multi-Jurisdictional Capability* function, the CAD system:

- *[Shall/Should]* have the ability to create a CFS event for user-defined multi-agency events and route the CFS event to the appropriate agency dispatch position(s).
- *[Shall/Should]* have the ability to create a linked CFS event for each required agency and route the CFS event(s) to the appropriate dispatch positions when an event involves more than one agency.
- *[Shall/Should]* have the capacity to create a multi-jurisdictional response; for example, should Jurisdiction X determine that Jurisdiction Y resources are needed on the scene, the fire dispatcher *[Shall/Should]* have the ability to forward/copy the CFS event without re-entering the event information to the appropriate Jurisdiction Y dispatcher based on CAD recommended or dispatched units.

- *[Shall/Should]* provide the ability to create and route a CFS event for dispatch even though the event is in another jurisdiction.
- *[Shall/Should]* provide the ability to transfer an active CFS event to another agency without closing the CAD CFS event within the originating agency.
- *[Shall/Should]* provide the ability to link cross-jurisdictional events using agency-definable parameters.
- *[Shall/Should]* update the originating jurisdiction's CFS event information if the dispatcher in the receiving jurisdiction updates or supplements the event.
- *[Shall/Should]* have the ability to create agency-definable recommendations for cross jurisdictional responses and automated messaging based on user-definable parameters.
- *[Shall/Should]* provide the ability to identify other jurisdiction addresses and alert the CAD user with the jurisdiction's name and contact information.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

10 REPORTING & MONITORING

Reporting and monitoring are important components of a CAD system. Reporting functions should include the ability for the command staff to generate statistical, detail event and log reports, and may include some form of snapshot/incident replay as well. CAD systems should also have the capability to manage the workflow of the call takers and dispatchers to include training and testing functions.

Operational Examples

Reports

- A citizen makes a complaint to the communications center and fire department that a recent response to a house fire was too slow, resulting in significant damage. The citizen threatens to file a lawsuit charging the communications center with malfeasance. The supervisor generates the following reports in the CAD system: a detail report for the incident in question showing a call-to-dispatch time of 1:15; a statistical average report showing a call-to-dispatch average of 1:47; and, a log report showing that the caller initially provided the wrong address, delaying the response. Additionally, a review of the entire incident/event history, including FD responses on their MDCs, shows that the responding units could not have responded any quicker. Based on these reports, the citizen withdraws the complaint.

Manage Workflow

- A dispatcher is handling all law enforcement radio traffic and calls for a rural county and a small town within the county. Earlier in the day, an armed robbery occurred in the town and a BOLO for a green van suspect vehicle was issued. Several law enforcement units are currently working various incidents. A county officer suddenly notifies the dispatcher that she is in pursuit of the suspect vehicle. The dispatcher needs to focus on the pursuit, so the supervisor logs into CAD and takes over dispatch responsibilities for the law enforcement units not involved in the pursuit.

10.1 Dispatch Supervisor Support



The CAD system should provide the supervisor with the ability to monitor the activity on any dispatcher workstation. If necessary, a supervisor needs to have the ability to take direct control over a dispatch position remotely, without leaving the supervisor console.

Sample Requirements

In order to support the *Dispatch Supervisor Support* function, the CAD system:

- *[Shall/Should]* provide the ability for a CAD supervisor, or another dispatcher with appropriate system permissions, to observe the activity of a given dispatcher including the pending events queue, active events, available units list, and map.
- *[Shall/Should]* enable a supervisor, or another dispatcher with appropriate system permissions, to co-dispatch the units under the control of another dispatcher.
- *[Shall/Should]* have the ability to add additional dispatchers “on-the-fly” for one or more services (law enforcement, fire service, and/or EMS), either globally or for predetermined geographical areas.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

10.2 CAD Management Reporting



It is essential that the CAD system include standard reports that can be run using a variety of flexible parameters. New reports should be defined either through the CAD system or a third-party reporting tool, and then should be stored as a standard report available through the CAD system.

The functionality needs to include the ability to report any data element by any other data element in the system. This may also include the ability to export data for use in third-party tools. A wizard may be provided that allows for user-generated reports.

Examples of typical CAD reports include the following reports that can be run by user-defined date and time range:

- Activity analysis
    - By day and hour
    - By day of the week
    - By hour of the day
    - By specified geographical area and by time period
- Attempted breaches in security
- Daily log showing all incidents received for the prior 24 hours from time of printing
- Delay reports (*e.g.* within dispatch, by unit from 'notified to en route', 'en route to arrive scene')
- Incident summary by specified geographical area and by time period
- Response time analysis
    - By incident type
    - By specified geographical area and by time period
- Time consumed
    - By day of the week and hour of the day
    - By incident type by hour of the day
    - By specified geographical area and by time period
- Workload activity
    - By group
    - By resource
- Snapshot / Scenario / Incident replays (see Section 10.4)

Error messages should be available for identifying system problems. Customizing reports to meet department needs should also be an option.

Sample Requirements

In order to support the *CAD Management Reporting* function, the CAD system:

- *[Shall/Should]* include standard reports that simultaneously use date, time, location, and/or incident type search parameters for report definitions.
- *[Shall/Should]* include the capability of customizing standard reports and for creating user-defined reports.
- *[Shall/Should]* provide access to all reports to the user, subject to permissions, from within the CAD system.
- *[Shall/Should]* include reports in the CAD security/permissions function (*i.e.* individual reports can be made available/unavailable based on a user's security profile).
- *[Shall/Should]* provide all reports to users, subject to permissions, regardless of the application used to create user-defined or custom reports (*i.e.* internal to the CAD system or via a third-party reporting or analysis tool).
- *[Shall/Should]* provide an *ad hoc* reporting capability.
- *[Shall/Should]* provide a data exporting capability.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

10.3 Training and Testing



This function relates to the necessity of having a training and/or testing CAD system environment that is isolated from the production environment for the purposes of program testing and file maintenance testing, as well as training of new personnel. This function is often referred to as a *CAD training mode*.

To the greatest extent possible, the training environment should be identical to the production region, thus allowing accurate testing and training to occur without impacting the production environment. The following are examples of the types of items to include in the training environment:

- Definition of the types of agencies being utilized (*i.e.* law enforcement, fire, EMS);
- Tables defined, to include unit names, recommendation patterns, premises information, personnel information, security permissions;
- Separate test E9-1-1 connection or a canned script of E9-1-1 information;
- Separate test mobile connection or a canned script of mobile information; and,
- Access to audible radio transmissions.

By having the training environment established and defined, the agency can develop a robust training program that simulates the live environment, to include the associated interfaces and radio traffic. The personnel can enter incidents and "mock" live incidents that are occurring on the radio without the production environment data being affected.

The training environment should have its own start-and-stop sequence that is independent of the production environment. The training environment does not have to be active at all times and can be started as needed.

Additionally, any programmatic change or changes to file maintenance records can be thoroughly tested and any issues resolved prior to being implemented in the production environment.

Sample Requirements

In order to support the *Training and Testing* function, the CAD system:

- *[Shall/Should]* include a training environment that accurately mirrors the live environment, including all tables and administrative configurations, and allows for call takers and dispatchers to train on specific services (*i.e.* law enforcement, fire service, and/or EMS) and on pre-configured geographic areas identical to that of the live environment.

The CAD system's training environment:

- *[Shall/Should]* be clearly identifiable as the training environment (*e.g.* "TRAINING" prominently displayed on the screen).
- *[Shall/Should]* have a separate E9-1-1 test connection or canned script E9-1-1 information and provide realistic training regarding incoming E9-1-1 data.
- *[Shall/Should]* be able to be used, operated, started up, shut down, and updated to match the live application without affecting the live environment.
- *[Shall/Should]* be able to be used to test modifications and updates to the live CAD application prior to implementing the modifications and updates in the live environment.

  Some larger PSAPs may maintain a separate test environment for application development staff that is independent of the training environment.

- *[Shall/Should]* have a separate E9-1-1 test connection or canned script E9-1-1 information (*i.e.* wireline, cellular, no record found, and VoIP) and *[shall/should]* provide realistic training regarding incoming E9-1-1 data.

The provider(s):

- *[Shall/Should]* provide initial and ongoing maintenance costs for the CAD training environment (and separate test environment if requested by the agency) in the proposed system cost section.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

10.4 Snapshot / Incident Replay



Training, quality review and investigations may be made easier for supervisors if the CAD system can capture and display an application *snapshot* of the entire dispatch center's system at the time a dispatcher assigned units to each incident. The snapshot may record the CAD-recommended dispatch, in addition to the complement that was assigned by the dispatcher. This snapshot could include items such as:

- Detailed list of current unassigned and assigned events, including: incident type, address, zones/beats, assigned units (for assigned events), unit recommendation
- Detailed list of all in-service units, including: assigned incident, location, status
- Detailed list of communications center staff, including: logged on call takers, dispatchers and their assignments, and supervisors
- List of units not in service

For auditing purposes, CAD systems typically include logs of events, actions, and sometimes even individual keystrokes in the system. *Incident replay* is a function that utilizes these logs to "recreate" a previous time segment such that a supervisor or investigation can observe a replay of the sequence and timing of a CAD event. In addition to investigations, this function is also very useful for training purposes.

Sample Requirements

In order to support the *Snapshot / Incident Replay* function, the CAD system:

- *[Shall/Should]* include functionality to provide a detailed, system-wide snapshot report and/or graphic display of the system status to include all units and events, based on a user-specified date, and time and an incident replay, based on a user-specified date and time, specific incidents, or other CAD events.

Relevant Technical Standards / Guidelines

- None at this time (see Section 1.5 for information on pending updates).

11 INTERFACES

An interface is the means by which the CAD system communicates information with other systems within the PSAP, such as E9-1-1 systems, or with external systems, such as federal databases, fire toning systems, or emergency operations centers (EOC). Typically, interfaces serve to provide CAD operators or first responders with a greater degree of information to increase situational awareness and officer safety through the addition of messaging or alerting capability that is not inherent to the CAD application itself.

To achieve that, CAD systems should interface to a broad range of internal and external systems. These systems include traditional subsystems, such as E9-1-1, federal, state, and local data warehouses, and RMS, as well as emerging technologies, such as video management systems, text messaging, and other multi-media systems.

These interfaces: enable the information exchange required for extended incident and resource management; as well as, facilitate some of the functionality within the CAD system, such as the automatic querying and capturing of license plate data as part of a field-initiated incident process or the ability to automatically send incident data to a "rip and run" printer in a fire station as part of the dispatch process.

Today, CAD interfaces most commonly communicate using TCP/IP protocols, although some legacy systems also use asynchronous serial connections and other forms of direct-connect methods to transfer data between the external system and the CAD system.

- For a detailed listing of CAD interfaces, see the *Priority Data Exchanges for Local Communications Centers* document available at: http://www.ijis.org/_publications/proj_reports.html.

> Practitioners and industry should strive to utilize standardized methodologies for the interface wherever possible. Interfaces conforming to national models, such as National Information Exchange Model (NIEM)[16] and GRA, and standards, such as the Automated Secure Alarm Protocol (ASAP) and the Nationwide Suspicious Activity Reporting Initiative (NSI), are designed to promote interoperability as well as save time and cost.

Operational Examples

- A law enforcement unit requests a vehicle license plate check on an out-of-state vehicle. The dispatcher, via the NCIC interface/function, runs the plate number/state through NCIC and advises the unit of the results (*e.g.* registration information, stolen status)
- A call-taker receives a CFS but, based on the geo-validation results, determines the call is actually in the neighboring jurisdiction. The call-taker sends the CFS to the other jurisdiction's CAD system via a CAD-to-CAD interface.
- A CFS is suspicious based on the national Suspicious Activity Reporting (SAR) guidelines, but the suspicious activity is not located by the responding unit and no report is created in the RMS. As the only information available is contained in the original CFS in the CAD system, the dispatcher flags the SAR submission, or the CAD system automatically does so based on its configuration,

[16] For more information on NIEM, visit: https://www.niem.gov/Pages/default.aspx

and the CFS event information is forwarded to the agency intelligence unit or Fusion Center via the SAR interface.

11.1 Essential Interfaces



At a minimum, all CAD systems should include the capability to interface to four subsystems: *E-9-1-1*, *regional external databases*, *messaging systems*, and *RMS*. Some agencies may consider the interface to mobile data computers (MDC) essential as well (see Section 11.2).

1) *E9-1-1*—An interface that imports subscriber information (ANI and ALI) for each E9-1-1 caller, as provided by the telephone company, into CAD-compliant entry process, eliminating the need for redundant data entry. If GIS data (latitude/longitude) is provided by the telephony provider, then the E9-1-1 data can be simultaneously imported into the mapping system for immediate centering and display.
2) *External Databases* (*i.e.* federal, state, NCIC, local)—Query to state, local and national databases. Queries to the state, local, RMS, and national databases will automatically occur from selected CAD commands using the messaging system interface. In addition, the operator (*i.e.* dispatcher or officer) will have the ability to use stand-alone query windows, eliminating redundant data entry. Responses to such queries should be stored with the incident record.
3) *Messaging Subsystems* (*i.e.* radio, paging/toning, email, text messaging)—Provides the ability to communicate with external messaging subsystems. This is one of the most important interfaces in terms of situational awareness and officer safety. Common examples include SMTP (email protocol), SMS (paging and text), and other TCP/IP-enabled technologies. Also common are interfaces to alerting modules, such as systems utilizing the existing radio network or an IP-enabled network (WAN/LAN), and text-to-voice technology to read CAD incident data over open intercom systems in fire/EMS stations.
4) *Records Management Systems*—Ideally, the RMS will have a robust interface designed to work in conjunction with the CAD application to enable a higher level of information sharing and workflow capabilities. In the absence of such an integrated solution, incident and resource data should be able to be sent to the RMS at configurable points in the incident management process (*e.g.* initiation, on-scene, clear). Additionally, the interface should be a two-way interface that enables the queries of incident and resource data by operators working in both applications. In addition to incident and resource information, RMS interfaces could include information/data on persons, premise, hydrants, inspection, training, personnel, roster, and/or logistics.

Sample Requirements

In order to support *E9-1-1 Interfaces*, the CAD system:

- *[Shall/Should]* enable incoming E9-1-1 ANI/ALI data to be automatically mapped to corresponding address and phone data fields based on the Master Street Address Guide (MSAG) standard in the CFS event entry form.
- *[Shall/Should]* support all E9-1-1 ANI/ALI formats including wireline, WPH1 and WPH2, VoIP, and Multi-Line Telephone Systems (MLTS).
- *[Shall/Should]* enable the capture of additional fields captured in the CFS event, including ESN, call type (landline, wireless), and ANI/ALI tracking ID (if available).

- *[Shall/Should]* use GIS data, if available, to extrapolate the closest geographical attribute (address, intersection, common place).
    - The radius used to extrapolate the closest geographical attribute *[Shall/Should]* be a configurable item within the system.
    - If GIS data is used to create the caller location, then the offset used to determine the approximate location *[Shall/Should]* be displayed.

In order to support *External Database Interfaces*, the CAD system:

- *[Shall/Should]* provide configurable query forms and response displays and be able to be custom-built to accommodate different federal, state and local database protocols.
- *[Shall/Should]* provide authorization to perform various queries, and the ability to read responses definable by the individual agency and by role to the field level.
- *[Shall/Should]* allow users to submit queries either with the query form or the command line (if applicable).
- *[Shall/Should]* allow users to automatically submit queries for persons and vehicles as part of other data entry processes, such as CFS event creation.
- *[Shall/Should]* enable the query request type and the database(s) to be queried to be specified from a predefined list, with automatic narrowing of pertinent databases based on user data input.
- *[Shall/Should]* provide intelligent updating of the query forms based on other CAD forms that contain person or vehicle data.
- *[Shall/Should]* provide a capability for entering new information into the selected external database(s) provided the external database(s) allow updating.
- *[Shall/Should]* provide a method for multiple queries to be submitted through a single form or command. This is sometimes referred to as *query spawning* or *cascading*.
- *[Shall/Should]* make query responses accessible either through the query response form or from the command line and *[shall/should]* be associated with a query response type.
- *[Shall/Should]* allow users to submit new queries based on data in the query response to logical links; and, *[Shall/Should]* also reference attachments that are associated with the response, which can be downloaded and viewed. Ideally, CAD will provide the capability to view common industry-standard multimedia file-types.
- *[Shall/Should]* provide the capability to alert dispatchers, PSAP supervisors, and street-level supervisors of “Hot Hit” responses to queries made by officers in the field, or data run that exists elsewhere in the CAD system (*i.e.* in a CFS event).
- *[Shall/Should]* provide optional audible and visual alerts that can be configured by the system administrator.
- *[Shall/Should]* log all queries and their responses (when permitted) for audit purposes.
- *[Shall/Should]* provide the ability to configure alerts for queries run by unauthorized personnel or devices, as well as the ability to monitor multiple queries of the same data or specified data.

Most CAD systems have an internal messaging system, and should provide the capability for workstation-to-workstation messaging; however, messaging to external systems/programs—Microsoft Outlook, mobile messaging, paging systems, and other text-based messaging—will require an interface.

In order to support the *Messaging Subsystem Interfaces*, the CAD system:

- *[Shall/Should]* be capable of TCP/IP communication, using industry-standard messaging protocols such as SMS and SMTP.
- *[Shall/Should]* provide the capability of pre-formatted messages, especially to paging and other handheld devices.
- *[Shall/Should]* create (automatically) an alphanumeric page for selected CAD incidents.
- *[Shall/Should]* allow a dispatcher to initiate an alphanumeric page for any paging group.
    - The information sent in the page *[Shall/Should]* be configurable by the agency and *[shall/should]* generally contain the incident number, type of incident, and location of the incident.
- *[Shall/Should]* provide an administrative mechanism to define paging groups.
- *[Shall/Should]* include multiple message types, including email, BOLOs, notifications, tactical command chat rooms, and others.
- *[Shall/Should]* provide a capability to format and send messages using just-in-time information, such as incident dispatch information, BOLOs or emergency weather alerts, and configurable triggers for these messages (*e.g.* incident type, assigned resources or location) for configurable recipients (*i.e.* send the chief a page when a specific incident type occurs at a specified location).
- *[Shall/Should]* ensure that messaging interfaces make use of the CAD address book.
    - The CAD address book *[Shall/Should]* allow for defining the types of devices recipients are able to receive messages on; and, *[Shall/Should]* have the ability to define a default device, as well as what devices (one, some or all) to receive messages on by day/time/response mode.
- *[Shall/Should]* provide the ability to include attachments associated with the message that can be downloaded and viewed by operators and recipients. Ideally, CAD should provide a capability to view common industry-standard multimedia file-types.
- *[Shall/Should]* include an interface to public awareness messaging[17] systems.
- *[Shall/Should]* include an interface to reverse 9-1-1, emergency notification, community notification messaging, and other standalone systems available to be activated by the PSAP or through local emergency management.
    - The system maintains a list of all callers who have elected to be a part of this community alert system. An information message can be created. The system then calls, emails and

[17] *Public awareness messaging* is the ability to broadcast, publish and send messages to individuals or agencies that need to be aware of critical events—examples include Amber Alert, critical incident occurrences, utilities, transportation, hospitals, or the public at large via the Internet.

texts every person on the list and plays or transmits the voice message. There is usually not an actual interface between the CAD system and the reverse 9-1-1 system unless the call list is maintained in the CAD database. A web interface is an option to provide citizens with the ability to add their name to the call list for noncritical incidents.

Many CAD systems are part of a larger suite of products, and will be tightly integrated with the RMS; however, interfaces to third-party RMS should still be required in the event that an agency does not want to update its existing RMS environment, elects not to use the CAD provider's RMS module, or the RMS is not provided by the CAD provider.

CAD-to-RMS interfaces can be one-way or two-way (unidirectional or bi-directional).

In order to support a *one-way CAD-to-RMS interface*, the CAD system:

- *[Shall/Should]* provide CAD incident and resource information to the RMS for use in reporting and case management.
- *[Shall/Should]* be a data push triggered by definable incident elements, such as incident status, incident disposition or manual submission by a dispatcher and/or call taker.

In order to support a *two-way CAD-to-RMS interface*, the CAD system:

- *[Shall/Should]* allow the user to view and manage data provided by the RMS from within the CAD application through a hyperlink or other means; for example, when a CFS event is created, the CAD system may receive an alert from the RMS that data related to a person, location, or vehicle is present in the system. Alternatively, attachments such as photos or video *[Shall/Should]* also be available to CAD users through a download or attachment to the CFS event.
- *[Shall/Should]* enable CAD users to be configurable by agency and role to the field level (and vice versa).
- *[Shall/Should]* provide (optional) a mechanism to create, record and otherwise manipulate a report number (separate from the CAD incident number) for cross-referencing purposes in the two systems.

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra

Several CAD-related reference interfaces were created by the LEITSC Project and are available on the ICAP website at:

- *International Association of Chiefs of Police (IACP)* – http://www.theiacp.org/Technology/OperationalTechnologies/CADRMS/tabid/831/Default.aspx

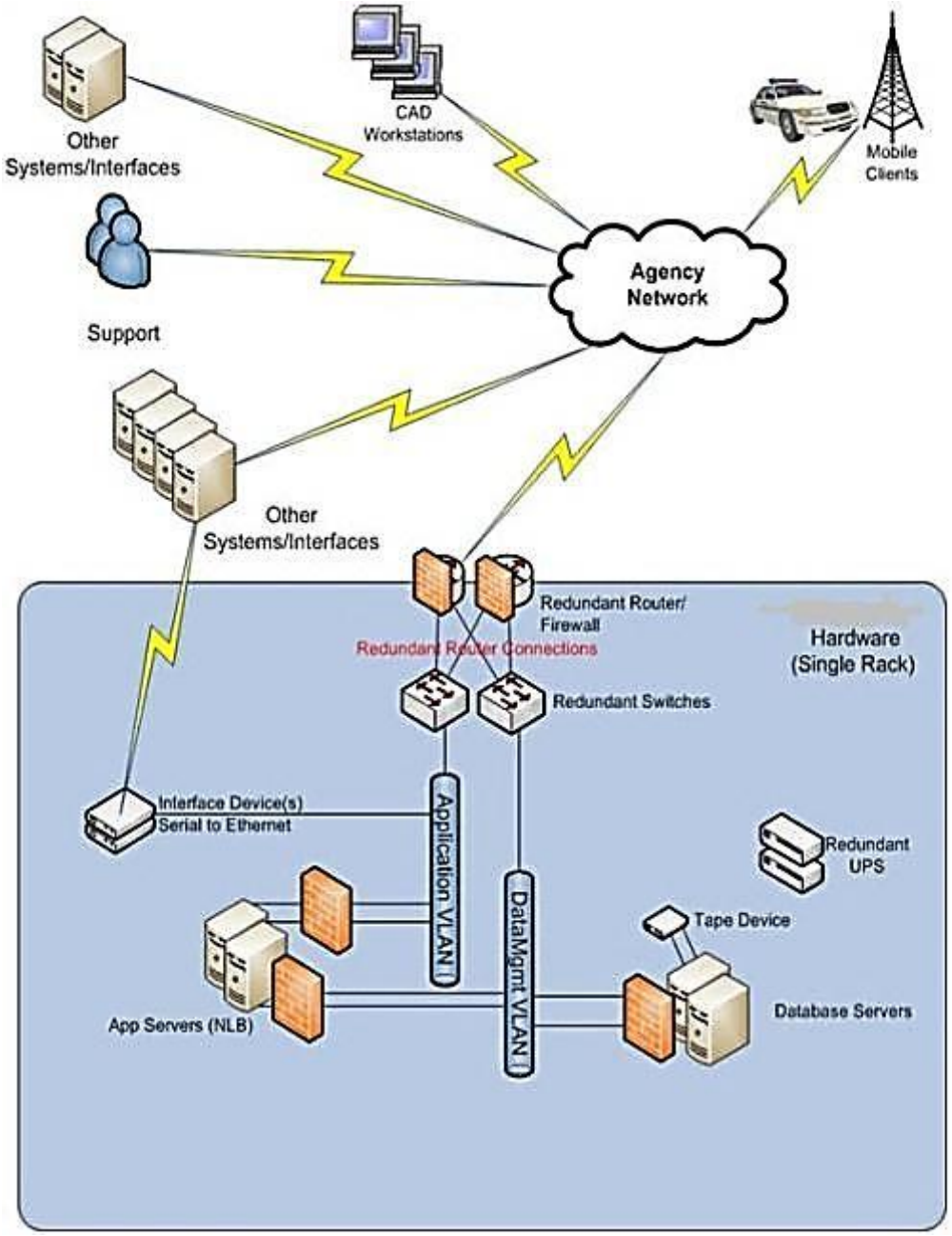
11.2 Additional Interfaces



It is often desirable to have a direct interface between the CAD system and other key law enforcement systems, such as other CAD systems in the area, alarm systems, and MDCs (if the system does not have an integrated mobile solution).

- *CAD-to-CAD*—Typically allows a single CAD system to interface to one or more CAD systems. The interface will support the ability to send or receive a CFS upon creation. Updates to CFS information, either field updates or comments will be exchanged through the interface for management by any system involved. The systems may also exchange unit status information. The data structures of the supported transactions should be NIEM conformant.
- *Mobile Data Computers*—Provides an extension to the CAD dispatch services from law enforcement vehicles, fire department rigs, and ambulances. Many modern CAD systems have a tightly integrated mobile module delivered as part of a suite of products; however, interfaces to third-party mobile data providers may still be required in the event that an agency does not want to update its existing mobile environment, elects not to use the CAD provider's mobile computing module or one is not provided by the CAD provider. The CAD system should interface with one or more mobile communications infrastructures to which the mobile units are attached, and should be able to be configured to meet the needs of the agency that it being served; for example:
- Law enforcement will require forms and functions to enable the querying of external databases.
- Fire rigs will require the ability to access pre-plan data and information (either locally or over the internet) regarding chemicals at a location.
- Ambulance crews will require forms and functions related to the management of patient data and medical procedures.

FIGURE 4. NETWORKING WITH ADDITIONAL INTERFACES



Sample Requirements

In order to support *Additional Interfaces*, the CAD system:

- *[Shall/Should]* provide access to MDC functions authorized to the field level within each function by system administrations down to the role level (*i.e.* a patrol officer may not have access to some functions that a street sergeant may have).
- *[Shall/Should]* be capable (depending on agency policy) of providing silent dispatch orders to a mobile unit, in addition to providing the unit with details of the CFS event, pre-plan information, patient information, premises history information, and other types of relevant information.

- *[Shall/Should]* enable the mobile unit to, if authorized, self-initiate incidents, self-dispatch incidents from a queue, change its status, query CAD and RMS information, and query local and national databases, such as wanted-person checks. Many MDCs, especially those not integrated as part of a CAD system, will require a message switch to enable the transmission of data and access to external databases.
- *[Shall/Should]* be able to have summary incident and resource monitoring capability.
- *[Shall/Should]* provide the ability for street supervisors in multi-agency, multi-jurisdictional environments to choose what agencies or areas within individual agencies they wish to monitor.
- *[Shall/Should]* provide the ability for CAD users to drill down into the details of summary incident and resource data, and have the ability to configure what data is displayed, as well as how it is displayed in terms of layout, font, font size, and colors.
- *[Shall/Should]* provide a day/night mode for mobile users.
- *[Shall/Should]* provide an integrated mobile mapping client.
- *[Shall/Should]* provide incident and resource management and monitoring capabilities through the in-car mapping solution.
- *[Shall/Should]* provide the ability to view real-time AVL data for user-selected units from the mobile client, and the ability to interact with the units identified on the map display.
    - This capability *[Shall/Should]* include messaging and other unit-related functionality.
- *[Shall/Should]* provide drive directions from the current location to a dispatched incident (or any selected location).
- *[Shall/Should]* provide mobile search capability for resources and personnel by type of vehicle, status and location.
- *[Shall/Should]* enable mobile users to search for incidents and locations.
- *[Shall/Should]* interface to [*insert specific application/product here*] Automated License Plate Reader (ALPR) software.

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

> While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra

11.3 Locational Systems Interfaces



Locational systems provide automated access to address, geographic and mapping information for public safety agencies. The primary locational systems include AVL, GIS, mobile and real-time mapping, and device mapping. These systems provide historic data that can be used in geospatial and temporal analytics. Very large jurisdictions may utilize interfaced, external resources, such as a spatial data warehouse for some GIS-related processing.

AVL

The CAD system will accept input from an AVL system. CAD converts the resource geographical location (*i.e.* X,Y coordinates) to a street address, records the vehicle's location in the unit history, and automatically performs a change of location for the vehicle resource, if necessary.

Some providers have started to refer to AVL as ARL (Automatic Resource Location) because it is no longer confined to providing the location of vehicles alone. CAD systems should accept geographical location from resources other than vehicles, such as handheld computing devices, mobile phones, or GPS-equipped radios.

GIS

The CAD system will interface with the jurisdiction GIS to support maintenance of: the CAD map; the law enforcement, fire department or ambulance; other map layers, such as reporting districts/areas; and, will also support the creation of the CAD geofile.

Modern CAD systems have a tightly integrated mapping application for use in CAD, mobile and RMS environments; however, if the CAD provider does not provide such an application, it will be required to interface to an external application.

Using the jurisdictional GIS information and the public safety agency or other map layers, the dispatcher has a tactical view of the city and/or dispatch area. The map can be controlled by specific CAD commands, such as zoom-and-pan, or preset commands, such as zooming to the address of a selected incident. The dispatcher can map/view all units and open incidents for an area or the city. Units and incidents are labeled on the map.

Device Mapping

Many devices, such as cell phones, smartphones, laptops, and portable radios now provide reporting of geographical location (*i.e.* X,Y/Z coordinates). These devices typically use similar functionality as AVL but with different business processes.

GIS-Driven Crime Analytics

These systems should provide data that allows for geospatial and temporal analytics. Analytics should support the tactical, strategic and administrative goals of the agency(s).

Sample Requirements

In order to support *Locational Systems Interfaces*, the CAD system:

- *[Shall/Should]* interface with existing state GIS.

- *[Shall/Should]* have a seamlessly integrated computerized map, which is a digitized map (GIS database) supporting Tactical Map Display (TMD).
- *[Shall/Should]* contain a map-centric TMD, in which the GIS/map is fully integrated with the CAD system.
    - In the case of a separate TMD application linked to the CAD system, the TMD *[Shall/Should]* support the automatic display of units as derived from an AVL system.
- *[Shall/Should]* integrate with aerial imaging technologies to provide digital, oblique, aerial imaging.
- *[Shall/Should]* link high-resolution aerial photos to mapping systems; overlay shape files directly on top of both oblique and/orthogonal images; and, display vector data.
- *[Shall/Should]* enable users to obtain measurements such as distance, height, elevation, and area directly from the 3D imagery, as well as insert GIS content and other data.
- *[Shall/Should]* include geographic data to support, at a minimum, the following:
    - System and boundaries registered to the street centerline in the geofile
    - Boundary assignments (*i.e.* determining the response zone for each incident) completed in real time by processing the incident's X,Y coordinates against the RCL and boundary files to determine the incident's location and response zone
    - Parcel-level GIS information, in which the approximate location of the front door of all the parcels in the state are stored in the geofile
    - Address validation and to determine an incident's location
    - Bulk data uploading
    - Weekly data updates
    - Metadata
    - FGDC standard format feed, like XML (eXtensible Markup Language) and KML (Keyhole Markup Language).

In order to support the *geofile system*, the CAD system:

- *[Shall/Should]* provide geo-fencing, and add the capability to establish law enforcement on-the-fly response zones, fire response areas, ambulance (EMS) response areas, street networks, and other geographical layers using typical mapping/GIS tools.
- *[Shall/Should]* support valid MSAG names and multiple "aliases" for street names, intersections, commonplace names, landmarks, and street or highway route numbers.
- *[Shall/Should]* stem geographically sensitive hazards, dispatch policies, and other system functions from validated locations.
- *[Shall/Should]* initiate a location verification step to add the coordinates of the incident location to the event and display an incident icon on the TMD as the CFS event is created.
- *[Shall/Should]* make a duplicate event check based upon the location and/or coordinates of the event, during the CFS event creation process.
- *[Shall/Should]* notify the event entry position via a prompt and show a list of the potential duplicate(s) if, during event creation, a potential duplicate event in the area is found.

- *[Shall/Should]* have a parameter (modifiable by the system administrator) specifying the distance in number of feet or other unit of measurement, from the location of the incident for duplicate checking.
- *[Shall/Should]* define location databases such as hazards, general premises information, street closures, and other user definable databases.
- *[Shall/Should]* perform a distance search to identify the existence of location information (*e.g.* hazards) during the event creation process.
- *[Shall/Should]* support different search distance criteria for different types of locations.
- *[Shall/Should]* support coordinate-based operations; *[Shall/Should]* be capable of full integration with a GPS-based AVL system; and, *[Shall/Should]* be capable of accepting named standards driven GPS reporting devices, such as GPS-enabled smartphones and portable radios.
- *[Shall/Should]* allow the system administrator to be able to modify parameters.

In order to support the *AVL system*, the CAD system:

- *[Shall/Should]* seamlessly integrate with the CAD system and provide detailed, accurate, real-time vehicle tracking.
- *[Shall/Should]* include the AVL ID (represented as an alias) for each unit user's status.
- *[Shall/Should]* include the indication that AVL is enabled for each unit on the user's status window. AVL can also be used for reporting, messaging, response and alerting functionalities.
- *[Shall/Should]* include a visual indication if units displaying on the map and in the queues are AVL equipped.
    - The visual indication if units displaying on the map and in the queues are AVL equipped *[Shall/Should]* be customizable by the system administrator.
- *[Shall/Should]* be able to play back a unit's AVL travel history and see the unit icon move from location to location on a map window.
- *[Shall/Should]* be capable of integrating with the existing GIS database.
- *[Shall/Should]* have other interactive functionalities also available, such as the ability to create and view unlimited groups of vehicles.
- *[Shall/Should]* provide for an automated alert function.
- *[Shall/Should]* provide for an automated alert for when vehicle is out of service.
- *[Shall/Should]* provide the ability to determine and modify all such alerts.
- *[Shall/Should]* provide the following information on any unit suffering loss of GPS signal (*e.g.* vehicle stopped, vehicle shut off, loss of network signal, loss of GPS data):
    - Last known position
    - Time of signal loss
    - Time lapse since signal loss
- *[Shall/Should]* provide minimal AVL reports that include:
    - Complete activity detail for specific date range
    - Vehicle last stop/end time for date range

  - Exception reports including all events that triggered an alert
  - Vehicle first start/begin time for date range
  - Miles per day, stops per day, average and summaries per vehicle

- *[Shall/Should]* pass unit status information to the AVL system whenever unit status is changed.
- *[Shall/Should]* pass any changes in unit location information to the AVL system if unit location changes are generated within the proposed system (as opposed to the AVL navigation system).
- *[Shall/Should]* display AVL updates on the map within two seconds of their receipt from the AVL controller.
- *[Shall/Should]* should be able to dispatch the nearest appropriate unit based on its AVL location using an appropriate routing engine to make that determination.

In order to support the *map and GIS analysis systems*, the CAD system:

- *[Shall/Should]* support either directly or, through an easily invoked (*i.e.* seamless) third-party mapping tool, the creation of *thematic maps*[18]; for example, a map showing the relative crime rate in each law enforcement district/zone in a given county.
- *[Shall/Should]* support either directly or, through an easily invoked (*i.e.* seamless) third-party mapping tool, the creation of *automatic pin maps*[19]; for example, the system *[Shall/Should]* produce a map showing the location of all auto thefts that occurred in a given county during the last two months.
- *[Shall/Should]* support either directly or, through an easily invoked (*i.e.* seamless) third-party mapping tool, the creation of *spatial data aggregation*[20]; for example, generate crime rates by district statistics by aggregating individual crimes occurring in each district of the County.
- *[Shall/Should]* support either directly or, through an easily invoked (*i.e.* seamless) third-party mapping tool, the creation of *trend analysis/forecasting*[21].
- *[Shall/Should]* access other RMS informational files to accommodate the needs and requirements of the crime analysis function and display this information using "pin mapping" techniques.

In order to support *map integration and functionality*, the CAD system:

- *[Shall/Should]* validate all incident locations, whether obtained from an E9-1-1 controller or entered directly by the call taker for administrative line (ten-digit) calls, against the CAD system's geofile to provide, at a minimum, cross streets, response areas, map page and coordinate, legal street names, and zip code.

[18] *Thematic maps* are maps of geographic boundaries (*e.g.* response zones, law enforcement districts, neighborhood watch areas, fire box areas, company areas, etc.) that cover the entire state or geographic subset and that are color-coded or differentially shaded to reflect the data contained within each boundary.
[19] *Automatic pin maps* are maps displaying, through icons or other symbols, the location of specific occurrences in the state or geographic sub-area.
[20] *Spatial data aggregation* is the ability to aggregate extracted information drill down into more meaningful statistics.
[21] *Trend analysis/forecasting* is the ability to extract recent historical incident occurrences to trend and pattern statistics and, when possible, to forecast future activity and resource information, and link to external systems, messaging capabilities and others.

- *[Shall/Should]* allow for the manual processing of the incident location, in the event a location cannot be properly validated against the geofile, so that a CFS event can be created if the location has been confirmed or known to exist within the local jurisdiction.
- *[Shall/Should]* produce (automatically) a report of all incident entries that did not validate on a scheduled basis.
- *[Shall/Should]* save original E9-1-1 ANI/ALI information as part of the CFS event if the user changes the original information (*e.g.* the incident is not at the caller's location).
- *[Shall/Should]* allow for processing of non-validated locations and notify the dispatcher of the special address.
- *[Shall/Should]* identify the appropriate agency (*i.e.* law enforcement, fire and/or EMS), district, sector, reporting area, agency of jurisdiction, and any other geographic boundaries containing an address, once it has been validated.
- *[Shall/Should]* display the two nearest cross-streets.
- *[Shall/Should]* perform location validations/geofile lookups independent of the CFS event creation process.

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

> While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra

11.4 Administration Interfaces



The administration CAD interface assists the entire public safety team (*i.e.* dispatchers, call takers, and command personnel) in working together. The key interfaces include push-to-talk, master time, and resource scheduling system.

Typically, the system has the ability to factor in many of the departmental rules for scheduling personnel for regular assignments and for overtime. The interface with the CAD system may include the ability to

have one point of maintenance for the names and assignments of all personnel. An interface may also include the roll-call list for each shift change for dispatcher review and confirmation as units log on to the shift.

Sample Requirements

In order to support *Administration Interfaces*, the CAD system:

- *[Shall/Should]* have the ability to import and display the radio ID (and optionally the officer ID) information to the dispatcher by those keying mobile and/or portable radios.
- *[Shall/Should]* have the ability to interface and synchronize all servers and CAD workstations with the master time clock.
    - This ensures each workstation and server provides an accurate time stamp.
- *[Shall/Should]* provide the ability for the agency to schedule personnel, including communications center personnel and officers.
    - This application is sometimes found in the agency's RMS.

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

> While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra

11.5 Communications Interfaces



There are several communications-based interfaces that allow CAD-generated information to be transmitted to others via e-mail, messaging and the Internet.

Sample Requirements

In order to support *Communications Interfaces*, the CAD system:

- *[Shall/Should]* accept, depending on agency policy, non-dispatchable incidents across the Internet.

  - Incidents accepted across the Internet will be of a general nature, in which a case (report) number may be needed for insurance purposes. The case number is generated and recorded. The incident is recorded in the incidents/events history database for statistical reporting.

- *[Shall/Should]* page or text (automatically) a message to pre-defined recipients or groups of recipients based on the event type.
- *[Shall/Should]* provide the capability for a CAD operator (PSAP personnel or CAD users) to page, email, or text a message to pre-defined recipients or groups of recipients.

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

> While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra

11.6 Integration / Interfaces with Other Systems



Fire/EMS functionality may require additional integration with other systems. Data transfer categories include inbound, outbound, peer-to-peer, and/or query-response. Interfaces should be NIEM-conformant wherever possible—examples include: E9-1-1 (ANI/ALI), paging, cross-agency automatic dispatching, billing systems, web-based resources/two-way integration for ICS, weather, EOC, fire and security alarms, hazardous materials databases, hospital availability, fire station alerting, push-to-talk radio, AVL, and pre-populating electronic patient care report (ePCR) forms.

Other interfaces may include functions such as attaching multimedia links to CAD locations that go to web-based resources, closed-circuit television (CCTV) feeds, traffic camera feeds, building information, and Hazmat information. This may also include two- and three dimensional-bar coding, Universal Product Code (UPC) numbers, and inventory identification.

It is particularly important that records interfaces be compliant with their respective local, state, and federal reporting standards reporting standards. Examples of federal reporting standards may include:

- NIBRS and N-DEx for law enforcement records management;

- NFIRS for fire service records management; and,
- NEMSIS for EMS records management.

A final public safety CAD functional specifications document should also reference the Public Safety Data Interoperability (PSDI) Priority Data Exchange for Local Communications Centers and list, at a minimum, the highest priority exchanges:

- E9-1-1 Information to CAD
- Incident notification (initial) (to mobiles)
- New incident from another CAD system (CAD-to-CAD)
- External alarm information (ASAP)
- NG9-1-1 Information to CAD
- Transfer of Incident
- Incident notifications via telematics – AACN (*e.g.* crash, disabled vehicle)
- Updates to CFS events from mobiles
- New incident from a field unit
- GIS /AVL providing closest unit recommendation
- Broadcast media warnings and alerts

Another emerging allied technology system is automated patient tracking systems (PTS). The deployment of such systems will require tight integration with the host CAD system or systems in the case where a single PTS is used in a multi-CAD environment.

> Interoperability and integration capabilities are becoming more critical as time goes by; therefore, a general recommendation is offered: CAD systems should be designed in such a way as to support interoperability and ease of interfacing.

Sample Requirements

In order to support the *Integration / Interfaces with Other Systems* function, the CAD system:

- *[Shall/Should]* allow the agency direct access to the underlying system information stored in the database (ODBC, FTP, web services) for future interface configuration, as well as appropriate database and system documentation to support this access.
- *[Shall/Should]* provide a capability to flag a CAD call for submission as a Suspicious Activity and submit that call to the agency's intelligence/counterterrorism unit or designated Fusion Center. This interface must conform to the standards set forth by the NSI and contained in the *Functional Standard (FS) Suspicious Activity Reporting (SAR) Ver. 1.5*.
- *[Shall/Should]* interface to [insert specific application/product here] incident command software.
- *[Shall/Should]* interface to [insert specific application/product here] records management software.
- *[Shall/Should]* interface with alarm monitoring companies using ASAP. This interface must conform to standards contained in the *APCO/CSAA ANS 2.101.1-2008: Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) External Alarm Interface Exchange*.

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

> While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra
- NSI: *Functional Standard (FS) Suspicious Activity Reporting (SAR) Ver. 1.5.* – http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.
- APCO/CSAA: *ANS 2.101.1-2008: Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) External Alarm Interface Exchange* – http://www.apcointl.org/new/commcenter911/documents/APCO-CSAA-ANS2-101-1web.pdf.

11.7 National SAR Initiative Functionality



The *SAR Program* is designed to support the sharing of information about suspicious activity, incidents, or behavior (hereafter, collectively referred to as *suspicious activity* or *activities*) that have a potential terrorism nexus (see Figure 5 below).

FIGURE 5. DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY[22]

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION[11]	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

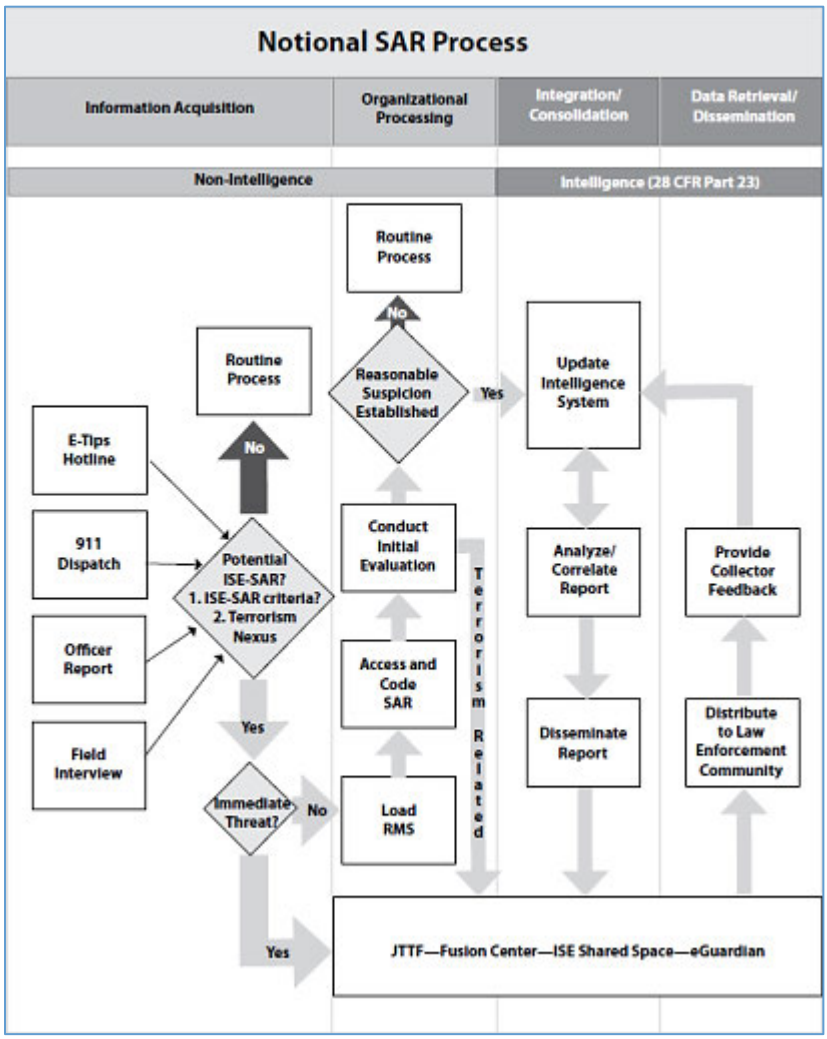
The program includes state and major urban area Fusion Centers and their law enforcement, homeland security, or other information sharing partners at the federal, state, local, and tribal levels to the fullest extent permitted by law.

In addition to providing specific indications about possible terrorism-related crimes, SAR reports can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, state or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among state and major urban area Fusion Centers and federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism.[23]

[22] Information Sharing Environment's *ISE-FS-200 v 1.5*, page 29, http://nsi.ncirc.gov/.
[23] Information Sharing Environment (2009). *Functional Standard (FS) Suspicious Activity Reporting (SAR) Ver. 1.5*.

Local information, determined and vetted to be SAR related by the local agency, is provided to the state-designated Fusion Center via a NIEM-conformant XML data exchange.[24] Both law enforcement RMS and CAD may have occasion to generate a SAR Report (see Figure 6 below).

FIGURE 6. NOTIONAL SAR PROCESS[25] [26]



An example of a SAR Report from CAD would be a CFS event of a suspicious person taking detailed photos (*e.g.* exits, security cameras) of a location deemed to be a critical infrastructure target. If the suspicious person is gone on arrival and there are no other witnesses to speak to or leads to follow, then a formal report is unlikely to result; however, this SAR, together with other SAR reports submitted to the

[24] To access the SAR Information Exchange Package Documentation (IEPD) search for "SAR" in the IEPD Clearinghouse at http://it.ojp.gov/default.aspx?area=implementationAssistance&page=1108.

[25] *Findings and Recommendations of the Suspicious Activity Reporting (SAR) Support and Implementation Project*, Oct 2008, page 24, http://nsi.ncirc.gov/

[26] Footnote 11 cited in Figure 5 reads, "These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions)."

Fusion Center, may assist investigators working on preventing terrorist activity. Alternatively, CAD functionality for SAR may be a flag to require an RMS report based on the type and location of the report (*i.e.* requiring a report for the scenario presented above).

Sample Requirements

In order to support the *National SAR Initiative* functionality, the CAD system:

- *[Shall/Should]* allow users to flag a CFS as "suspicious" with regard to the National SAR Initiative.
- *[Shall/Should]* send a "suspicious-flagged" CFS to an external application, database, or LE RMS that handles SAR reporting.
- *[Shall/Should]* provide the capability to notify an intelligence unit/counterterrorism unit when a SAR is submitted.

Relevant Technical Standards / Guidelines

- *Nationwide SAR Initiative Program Management Office (NSI PMO)* (includes links to: *SAR Fact Sheet*; *NSI Training*; *ISE-FS-200*, the *SAR Exchange Standard*; and, other relevant information) – http://ise.gov/nationwide-sar-initiative

11.8 Emergency Operations Center Interface



The operation of an emergency center requires the multidirectional exchange of information between CAD and the EOC. Units may be assigned to the EOC, at which point the EOC will take control of the unit until released. CAD will maintain the ability to monitor the unit availability status. CAD will continually update the EOC with incident information.

The EOC supports the ability to track resources and incidents that are related to a disaster situation. The Federal Emergency Management Agency (FEMA) requires that these resources and incidents be tracked in order to receive federal funding; however, the ability for incident commanders, agency command staff and EOC personnel to have a high level view of resource availability and incidents related to the event is critical in order to mitigate further deterioration of the event. Some EOCs will need the ability to dispatch incidents that require EOC direction; therefore, the ability for call taking and dispatching should be considered in any EOC plan. Another variable that may be considered is the ability to directly dispatch from the EOC to only a certain geographical area, only specific assigned units, or by specific incident types; however, this is not always necessary.

The support of an emergency may also require that the dispatch center be moved to an off-site, secure location; and, therefore, should include a hardware system and network connectivity that will support the creation of off-site, real-time backup at servers located at the EOC. Other functionality that can be provided by the CAD system in support of the EOC operations includes the remote CAD dispatching capability mentioned above and support for multiagency event coordination.

These two optional features provide benefits to the CAD system even if the dispatcher does not have to be moved. Multiagency event coordination requires that support agreements be negotiated and in place amongst all of the agencies.

CAD system data is a cornerstone of local, operational situational awareness that is critical for emergency management functions. CAD systems provide relevant information to emergency management software systems.

Sample Requirements

In order to support an *Emergency Operations Center Interface*, the CAD system:

- *[Shall/Should]* have an EOC viewable setting that can be initiated through a web viewer or license to allow the EOC to view incidents and units specific to the emergency event.
- *[Shall/Should]* allow for incident creation that is within the area of the incident but be limited to certain incident types depending on the type of disaster.
- *[Shall/Should]* interface to [insert specific application/product here] incident command software.
- *[Shall/Should]* allow for the allocation of certain apparatus/units that can be managed and dispatched out of EOC for a specific CFS (planned or unplanned) without negatively impacting the CAD system. It is also preferred that in this instance, none of the all activities will be manual (*i.e.* the system will keep track of all apparatus and personnel for both the agency wide response and the EOC response area).

Relevant Technical Standards / Guidelines

- *National Information Exchange Model (NIEM)* – www.niem.gov
- *Global Reference Architecture (GRA)* – www.gra.gov
- *Logical Entity eXchange Specifications (LEXS)* – http://www.lexsdev.org

> While NIEM, GRA, and LEXS would not necessarily apply to the internal workings of a CAD system, they have great relevance to the standardization and interoperability of information sharing exchanges in/out of a CAD system, and should therefore be taken into consideration for any public safety system's information sharing capabilities/functions.

Existing reference exchanges may be available at:

- *Information Exchange Package Documentation (IEPD) Clearinghouse* – http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Existing GRA-conformant service specifications may be available at:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra

12 FUTURE PIPELINE / ON THE HORIZON

This section presents basic information regarding other current or "on the horizon" efforts that have a great likelihood of affecting CAD functionality. The information provided is not intended to be definitive, as these are works in progress as of this writing. These are offered here so the reader can be on the lookout for these initiatives for future consideration and use.

12.1 Next Generation 9-1-1



NG9-1-1 will update and modernize the 9-1-1 service infrastructure in the United States to improve public emergency communications services in a wireless, mobile society. NG9-1-1 will enable additional communication media, as well as almost totally revamp the methods that are currently employed to route and deliver emergency calls to 9-1-1 service centers. In addition to calling 9-1-1 from a phone, the public will be able to transmit text, images, video, and data to the 9-1-1 service center. Landline-based phones will have their locations pre-validated, increasing the likelihood that they will be correctly routed to the proper 9-1-1 service center. GIS technology will be used to route calls to the proper dispatch center through a highly secure Emergency Services IP network (ESInet), rather than through traditional 9-1-1 trunk lines. Additional service responder types, such as poison control and Hazmat, will be supported in both a regional and local manner. Backup and failover availability will be driven by policies and seamlessly integrated with the ESInet. Extensive telematics type devices (*e.g.* personal health monitoring devices, accident detection devices) will also be supported under NG9-1-1.

To be compatible with NG9-1-1, CAD systems, at a minimum, will have to support the display, storage, retrieval, and forwarding to mobile data devices of the additional emergency-related media supported by NG9-1-1, such as text messages, images, telematics information, and streaming video and audio. Additionally, most CAD systems will have to support the geo-validation requirements and the EIDD employed within NG9-1-1.

- For more information, see *NENA 08-003: Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3*: http://www.nena.org/standards/technical/i3-solution

> Practitioners and Industry should watch for opportunities to take advantage of NG9-1-1 capabilities as they are rolled out by telecommunications companies and public safety technology providers.

EIDD

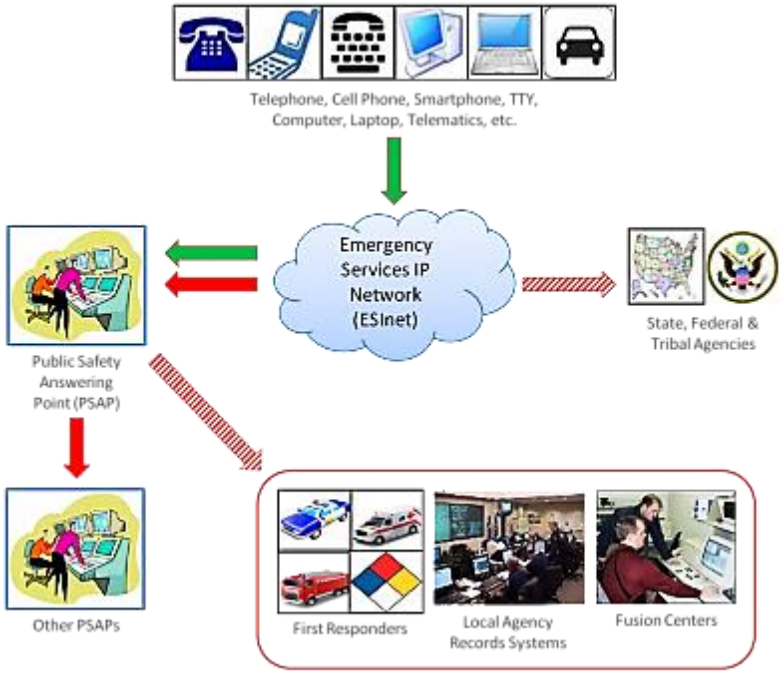
To support NG9-1-1 information sharing, the EIDD, a NIEM-conformant XML exchange standard, is being jointly developed by APCO and NENA. This exchange provides a standardized mechanism for exchanging emergency incident related data. It is being established to assist NG9-1-1 Functional Elements (FEs) exchange data, as required by the NENA i3 standard. Under i3, FEs may be pooled together and implemented in various combinations offered by different vendors. When these FEs interact with each other, they must pass data back and forth as specified in i3. The EIDD was created to support standardized incident data exchanges occurring between FEs manufactured by different providers and/or are geographically separated, including: CAD-to-CAD; CAD-to-RMS; and, CAD-to-another public safety entity.

APCO and NENA plan to take the EIDD through an ANSI-certified standardization process. As a standard, CAD systems should use the EIDD whenever incident related information must be passed to other FEs, including remote CAD systems and systems manufactured by different manufacturers.

Security and authentication are mandated in i3 and, by default, will be extended to implementation of EIDD-related transactions since EIDDs will often be used to exchange highly confidential information (*e.g.* emergency response resource locations, health related information). As such, CAD systems that plan to use the EIDD standard will most likely have to support the security and authentication requirements of i3.

Due to its robust capability, and being the recognized standard for exchanging NG9-1-1 information, the EIDD exchange standard will likely become one of the most widely used data exchange formats in public safety.

FIGURE 7. SIP[27] AND EIDD EXCHANGES FOR PUBLIC SAFETY[28]



Practitioners and Industry should watch for opportunities to take advantage of EIDD Exchange Standard as it becomes available. As a standard, it should lower cost for implementation and maintenance; and, the capability it will provide means increased interoperability. This will likely become a functional requirement for new CAD systems in the future.

NG9-1-1 Policy Routing Function

Next Generation 9-1-1 uses policies for completing a variety of functions including call routing, disaster recovery, and overload handling. The policies are controlled by a *Policy Routing Function (PRF)*. The *PRF* contains a policy store (database) that contains the NG9-1-1 policies used by the PRF functional

[27] *SIP Message* (green)—Carries the actual call data (*e.g.* voice, text messages, etc.) or references to where it is stored.
[28] *EIDD Exchange* (red)—The NIEM-conformant EIDD is the central link between the collection and distribution of all PSAP-generated NG9-1-1 data and its exchange between all other public safety communications systems. Other potential uses for the EIDD messages are red striped.

element. PRF FEs and their policy stores may be located at local PSAPs and at regional data centers that support and control the ESInet. The types of policies that are typically available at PRFs include:

- Policies that establish which service agency(s) should be assigned to an incident based on the operational status of the agencies capable of handling the incident, the incident's type, and the incident's location; and
- Policies that determine the Initial resource types and quantities to assign to an incident based on the incident's nature code, priority and locations (*i.e.* resource deployment plans).

CAD systems that operate within an NG9-1-1 environment will most likely need to access the PRF FEs and their policies to properly determine routing and other policy directed decisions; for example, incidents that are initiated at 9-1-1 centers, such as when a law enforcement officer discovers a structure fire while on routine patrol, need to have an agency assigned to handle them. The CAD system in which the incident was created must consult the PRF FE or its internal policy files to determine which agencies should be assigned to the incident.

NG9-1-1 compliant CAD systems may not have to directly use the policies available at the appropriate PRF, but they should be able to query the PRF to help decide what agency and what dispatchers and call takers should handle an incident. If the CAD system is not directly interfaced to the PRF, then a mechanism should be implemented to keep the internal policies used by the CAD system synchronized with the policies contained in the PRF; for example, policy updates to the PRF should automatically be downloaded to CAD in order to insure that the same policies are employed regardless of whether the PRF or the CAD system handles them.

NG9-1-1 Geo-Validation and Geo-Call Routing

NG9-1-1 uses GIS functions to validate and locate emergency calls for service. NG9-1-1 contains a Spatial Information Function (SIF) that stores the GIS data used by the i3 applications (FEs) of NG9-1-1. Data is replicated from the SIF to the i3 FEs that require GIS data, such as the Emergency Call Routing Function (ECRF) and the Location Validation Function (LFV), as well as to FEs that require GIS data in 9-1-1 centers.

It is critical that CAD uses the same GIS data as the ECRF in order to insure that the same incident routing decisions are completed regardless of whether the analysis was completed in CAD or by the ECRF. Otherwise, incidents may be routed to different 9-1-1 centers and assigned to different response agencies depending on whether the analysis is completed via the ECRF or CAD.

CFS are routed in NG9-1-1 by geographically determining which 9-1-1 center boundary and service area polygons contain the incident's location. This analysis is typically completed using a PIP analysis. NG9-1-1-compliant CAD systems should be able to use the incident's location (*e.g.* an X,Y coordinate) and a set of polygon boundaries representing response agency service areas (*e.g.* LE agencies, fire departments, EMS service areas) in a PIP analysis to determine what boundary contains the incident.

It is also critical that civic locations are validated using the same GIS data, regardless of whether the LVF or CAD complete the validation. A civic location (address) that is validated correctly by the LVF must also be validated by CAD. Otherwise, incidents from locations that are valid may not be assigned properly in CAD resulting in incorrect dispatch assignment and delayed emergency responses.

It is anticipated that, due to the various input methods of emergency call information enabled by NG9-1-1 (*e.g.* text messages, images, video, telematics, and various sensors), NG9-1-1 data is likely to enter the ESInet from a large number of locations requiring some method of determining which PSAP(s) to route the information, data, and calls to. The routing functions provide the information necessary for NG9-1-1-compliant systems to correctly route the information. These may become functional requirements for new CAD systems in the future.

12.2 Broadband / Long-Term Evolution



Public safety agencies and technology solutions providers have already begun to plan for the deployment of advanced wireless communications systems using the next-generation, all IP-based, broadband, wireless, LTE technology. The capabilities of LTE are anticipated to provide multi-path (primary and backhaul) wireless support to law enforcement, fire, and EMS agencies across all levels of government, to include data, voice and multi-media communications. In fact, several public safety agencies have already acquired and deployed capabilities in the third generation (3G) broadband environment as part of local community broadband initiatives. Given the capabilities and limitations of the 3G technology, many, if not most, will be seeking to migrate to LTE environments.

LTE, which will be deployed in 700 MHz band dedicated to public safety, supports a wide array of broadband communications features not supported by the narrowband communications systems used by public safety today; for example, through the use of LTE, video, high resolution images, and other multimedia, data can be exchanged among public safety personnel in the field and with backend systems and support personnel.

LTE networks will provide a number of new network services that will be useful for public safety applications and operations, including:

- Transmitting reliable and secure video, voice and data streams [with Quality of Service (QoS)] dynamically signaled during session setup and the ability to be modified mid-session);
- Determining the location of a mobile device and the accuracy of the estimated position;
- Supporting concurrent multimedia sessions, as well as allowing for the setting/changing of priority levels and QoS attributes of different information flows (voice, video, data) and sessions;
- Indicating network events (*e.g.* detecting devices that have just powered on, detecting devices which have just roamed into or out of a network);
- Geo-fencing event notifications (*e.g.* receiving notifications when mobile devices cross a predetermined region, setting of parameters that define geo-fenced regions);
- Determining device capabilities;
- Managing and defining user groups; and,
- Determining whether users in a group are currently attached to a LTE network.

It is anticipated that as the public safety broadband/LTE becomes readily available, the capabilities of the technology available to public safety will be dramatically enhanced. Watch for new functions and capabilities available from your technology providers.

13 MOBILE CAD FUNCTIONS

Although extremely important to public safety, the functionality extended by CAD to MDCs and PDAs used by law enforcement, fire, and EMS is out of the scope of this particular document. It is hoped that a future effort will address this topic; however, as a note to the reader, some typical mobile CAD functions include:

- Ability to update own unit status (*e.g.* en route, on location)
- BOLOs, notifications, alerts
- Call details
- Call queue (*i.e.* pending calls)
- Current call assignments
- Messaging (*e.g.* car-to-car, CAD-to-dispatcher)
- NCIC, local, state queries
- Premises information, including CFS history
- RMS queries
- Route/map information
- SOPs
- Warrant checks

14 APPENDICES

These references and links provide the reader with additional and/or in depth information regarding numerous related issues.

14.1 APPENDIX A – Related Standards Development Organizations (SDO)

- Association of Public Safety Communications Officials International (APCO) – http://www.apco.org
- Central Station Alarm Association (CSAA) – http://www.csaaul.org
- National Emergency Number Association (NENA) – http://www.nena.org
- National Fire Protection Association (NFPA) – http://www.nfpa.org

14.2 APPENDIX B – Related Models and Standards

Models

- National Information Exchange Model (NIEM) – http://www.niem.gov
- Global Reference Architecture (GRA) – http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015

Standards

- *NFPA 950: Standard for Data Development and Exchange for the Fire Service* – http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=950&cookie%5Ftest=1
- *NENA 56-004: TTY/TDD Communications Standard Operating Procedure Model Recommendation* – http://72.27.230.243/sites/default/files/NENAopsTTY-TDDSOP06252005Final.pdf
- *APCO 1.108.1-201x: Minimum Operational Standards for the Use of TTY/TDD devices in the Public Safety Communications Center* (in development) – http://www.apco911.org/911-resources/standards/apco-standards-in-progress.html

14.3 APPENDIX C – Global Resources

Global Standards Package (GSP)

Global's collection of normative standards have been independently versioned and assembled into a package of composable, interoperable solutions specifically supporting information exchange. This package is known as the Global Standards Package (GSP). GSP solutions are generally technically focused but may also include associated guidelines and operating documents. GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:

- *Global Reference Architecture (GRA)* – http://www.it.ojp.gov/globaljra/
    - Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- *Global Service Specification Packages (SSP)* – http://www.it.ojp.gov/globaljra/

  - Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.

- *Global Federated Identity and Privilege Management (GFIPM)* – http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179
  - Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
- *Global Privacy Technology Framework* – http://www.it.ojp.gov/default.aspx?area=privacy
  - A framework for automating access control (in particular, privacy) policy as part of information exchange.
- *Global Information Sharing Toolkit (GIST)* – *http://www.it.ojp.gov/gist*

14.4 APPENDIX C – Other Resources

- *Priority Data Exchanges for Local Communications Centers* – http://www.ijis.org/_publications/proj_reports.html
- *Guide to Information Sharing and Data Interoperability for Local Communications Centers* – http://www.ijis.org/_publications/proj_reports.html
- National Emergency Number Association (NENA) – http://www.nena.org/
- U.S. Department of Justice, Office of Justice Programs, Justice Information Sharing – http://www.it.ojp.gov

14.5 APPENDIX D – Previous Versions of CAD Functional Standards / Requirements

- Law Enforcement Information Technology Standards Council (LEITSC): *Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems* – http://www.theiacp.org/Technology/OperationalTechnologies/CADRMS/tabid/831/Default.aspx
- IJIS Institute: *Revision Assessment for the Incorporation of Fire and EMS Functions into the Law Enforcement CAD Functional Specifications* – http://www.ijis.org/_publications/proj_reports.html

14.6 APPENDIX E – Relevancy Matrix

Reference Number	Function	Law Enforcement	Fire Services	Emergency Medical Services
2.1	Call Taking	✓	✓	✓
2.2	CAD Incident / Event Types	✓	✓	✓
2.3	Update Call for Service Event Data	✓	✓	✓
2.4	Determine Dispatch Need	✓	✓	✓
2.5	Utilize Incident Disposition	✓	✓	✓
2.6	Assign Incident Classification and Priority	✓	✓	✓
2.7	Check for Duplicate Incidents	✓	✓	✓
2.8	Incident Information	✓	✓	✓
2.9	Determine Capture Locations	✓	✓	✓

Reference Number	Function	Law Enforcement	Fire Services	Emergency Medical Services
2.10	Location Verification	✓	✓	✓
2.11	Retrieve Incoming Calls	✓	✓	✓
2.12	Involved Person Information	✓	✓	✓
2.13	Involved Vehicle Information	✓	✓	✓
2.14	Premises Hazard and Previous History	✓	✓	✓
2.15	CAD Event Creation	✓	✓	✓
2.16	Determining Response Agency and Service Area	✓	✓	✓
2.17	Alarm Processing	✓	✓	✓
2.18	CAD Event Routing	✓	✓	✓
2.19	Ability to Route to a "Decision Dispatcher"		✓	✓
3.1	Run Cards / Response Plans	✓	✓	✓
3.2	Adjustable Dispatch Levels	✓	✓	✓
3.3	Additional Attributes	✓	✓	✓
3.4	Mutual Aid Function	✓	✓	✓
3.4	Automatic Aid Function	✓	✓	✓
3.5	Unit Rotation (Unit Load Balancing)	✓	✓	✓
3.6	Conditional Availability of Apparatus	✓	✓	✓
3.7	Special Dispatch Areas	✓	✓	✓
3.8	Emergency Medical Dispatch / Incident Triage	✓	✓	✓
3.9	Channel Designations	✓	✓	✓
3.10	Be On the Look-Out / Attempt to Locate	✓	✓	✓
3.11	Dispatch Units	✓	✓	✓
3.12	Resource Alerting	✓	✓	✓
4.1	Move-up ("Fill-in" and "Station Fill")	✓	✓	✓
4.2	Staffed vs. Unstaffed Units	✓	✓	✓
4.3	Cross-Staffing / Crew Counting / Shared Staffing Crew Accountability / Contingency Staffing	✓	✓	✓
4.4	System Status Management (Dynamic Resource Deployment)		✓	✓
4.5	Additional Unit Status	✓	✓	✓
4.6	Strike Team / Task Force Designations	✓	✓	✓
4.7	Rostering	✓	✓	✓
4.8	Scheduling	✓	✓	✓
4.9	Mileage Tracking	✓	✓	✓
4.10	Hydrant Location and Status		✓	
4.11	Additional Unit Dispositions	✓	✓	✓
4.12	Exception Reason Tracking	✓	✓	✓
4.13	Public Safety Flight Tracking	✓	✓	✓
4.14	Geo-Fencing	✓	✓	✓
4.15	Station Dispatch		✓	✓
4.16	Pre-Release or Pre-Alerting	✓	✓	✓
4.17	Vehicle / Unit Change	✓	✓	✓
4.18	Automatic Driving Directions / Routing	✓	✓	✓
4.19	Bypassed Units	✓	✓	✓
4.20	Post-Dispatch Response Re-evaluation	✓	✓	✓
5.1	Display of Incident / Event Data	✓	✓	✓

Reference Number	Function	Law Enforcement	Fire Services	Emergency Medical Services
5.2	Update Incident Status	✓	✓	✓
5.3	Dispatch Resource Decision	✓	✓	✓
5.4	Update Assigned Resources	✓	✓	✓
5.5	Update Supplemental Resources Tracking	✓	✓	✓
5.6	Assign Units	✓	✓	✓
5.7	Update Incident Data	✓	✓	✓
5.8	Assign Records Management System Incident / Case Number	✓	✓	✓
5.9	Transfer Basic Incident Data to Records Management System	✓	✓	✓
5.10	Display Additional Incident Data	✓	✓	✓
5.11	Reopen Incident	✓	✓	✓
5.12	Add Destination Locations	✓	✓	✓
5.13	Hospital Status / Availability and Hospital Recommendation		✓	✓
5.14	Patient Tracking	✓	✓	✓
5.15	Linking an Audio File to a CAD Event	✓	✓	✓
5.16	Multiple Simultaneous Incidents to a Single Unit	✓	✓	✓
5.17	Scheduled Events	✓	✓	✓
5.18	Secondary Incident Location	✓	✓	✓
5.19	Single Discipline Incident to a Combined Discipline Incident	✓	✓	✓
5.20	Timers	✓	✓	✓
5.21	User Defined Status Timers	✓	✓	✓
6.1	Request Supplemental Resource	✓	✓	✓
6.2	Request Supplemental Resource Rotation List	✓	✓	✓
6.3	Notify Supplemental Resource Service	✓	✓	✓
6.4	Enter and Update Supplemental Service Record	✓	✓	✓
7.1	Determine Incident / Event Status	✓	✓	✓
7.2	Utilize Incident Management	✓	✓	✓
7.3	Determine Report Functionality	✓	✓	✓
7.4	Record Disposition	✓	✓	✓
7.5	Send Data to Records Management System	✓	✓	✓
7.6	Assign Agency-Specific Report Numbers	✓	✓	✓
8.1	Geofile Maintenance	✓	✓	✓
8.2	Security	✓	✓	✓
8.3	Logging	✓	✓	✓
8.4	Configuration	✓	✓	✓
8.5	Table Maintenance	✓	✓	✓
8.6	Communications Center / PSAP Relocation	✓	✓	✓
8.7	CAD Catch-Up	✓	✓	✓
9.1	Notifications	✓	✓	✓
9.2	Contact List	✓	✓	✓
9.3	Premises Information / Hazards	✓	✓	✓
9.4	Communications Center / PSAP Standard Operating Procedure	✓	✓	✓

Reference Number	Function	Law Enforcement	Fire Services	Emergency Medical Services
9.5	Agency Specific Incident / Location / Unit Standard Operating Procedure	✓	✓	✓
9.6	Remote Access	✓	✓	✓
9.7	CAD Workstation-to-CAD Workstation Messaging	✓	✓	✓
9.8	Incident Command Support	✓	✓	✓
9.9	Narrative Field "Shorthand" (Auto Text)	✓	✓	✓
9.10	Command Line / GUI	✓	✓	✓
9.11	Date / Time Stamps	✓	✓	✓
9.12	Unit Status Transitions Matrix	✓	✓	✓
9.13	Single Sign-on for CAD and CAD Sub-systems	✓	✓	✓
9.14	Multi-Agency / Multi-Jurisdictional Capability	✓	✓	✓
10.1	Dispatch Supervisor Support	✓	✓	✓
10.2	CAD Management Reporting	✓	✓	✓
10.3	Training and Testing	✓	✓	✓
10.4	Snapshot / Incident Replay	✓	✓	✓
11.1	Essential Interfaces	✓	✓	✓
11.2	Additional Interfaces	✓	✓	✓
11.3	Locational Systems Interfaces	✓	✓	✓
11.4	Administration Interfaces	✓	✓	✓
11.5	Communications Interfaces	✓	✓	✓
11.6	Integration / Interfaces with Other Systems	✓	✓	✓
11.7	Suspicious Activity Reporting Functionality	✓	✓	✓
11.8	Emergency Operations Center Interface	✓	✓	✓

14.7 APPENDIX F – Acronyms and Abbreviations

Acronym or Abbreviation	Definition
3G	third generation
ACD	Automatic Call Distribution
ALI	Automatic Location Information
ALPR	Automated License Plate Reader
ALS	Advanced Life Support
ANI	Automatic Number Information
ANS	American National Standard
APCO	Association of Public-Safety Communications Officials International
APL	Automatic Person Location
ARL	Automatic Resource Location
ASAP	Automated Secure Alarm Protocol
ATL	Attempt to Locate
AVL	Automatic Vehicle Location
BJA	Bureau of Justice Assistance
BLS	Basic Life Support
BOL or **BOLO**	Be on the Lookout
CAAMTS	Commission for the Accreditation of Air Medical Transport Systems

ACRONYM OR ABBREVIATION	DEFINITION
CAD	Computer Aided Dispatch
CCTV	closed-circuit television
CFS	call for service
CJIS	Criminal Justice Information Services [FBI]
CLEC	competitive local exchange carriers
CPE	Customer Premises Equipment
CSAA	Central Station Alarm Association
DMV	Department of Motor Vehicles
DRE	Drug Recognition Expert
E9-1-1	Enhanced 9-1-1
ECRF	Emergency Call Routing Function
EIDD	Emergency Incident Data Document
EMD	Emergency Medical Dispatch
EMS	Emergency Medical Services
EOC	emergency operations centers
ePCR	electronic patient care report
ESInet	Emergency Services IP network
ESN	Emergency Service Number
ETS	Electronic Tracking System
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
FEs	Functional Elements
geofile	geographic file
GFIPM	Global Federated Identity and Privilege Management
GIS	Geographic Information System
GIST	Global Information Sharing Toolkit
GPS	Global Positioning Satellite
GRA	Global Reference Architecture
GSP	Global Standards Package
GUI	Graphical User Interface
Hazmat	hazardous material
HIPAA	Health Information Portability and Accountability Act
IACP	International Association of Chiefs of Police
ID	identification
IDLH	Immediately Dangerous to Life or Health
IEPD	Information Exchange Package Document
IP	Internet Protocol
IPP	Internet Printing Protocol
KML	Keyhole Markup Language
LEC	local exchange carriers
LEITSC	Law Enforcement Information Technology Standards Council
LFV	Location Validation Function
LPD	Line Printer Daemon
LTE	Long-Term Evolution
MCI	Mass Casualty Incidents
MDC	Mobile Data Computer

ACRONYM OR ABBREVIATION	DEFINITION
MLTS	Multi-Line Telephone Systems
MOU	Memorandum of Understanding
MSAG	Master Street Address Guide
NCIC	National Crime Information Center [FBI]
N-DEx	National Data Exchange [FBI]
NEMSIS	National EMS Information System
NENA	National Emergency Number Association
NFIRS	National Fire Incident Report System
NG9-1-1	Next Generation 9-1-1
NIBRS	National Incident Based Report System
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NISS	National Information Sharing Standards
Nlets	The International Justice & Public Safety Network
NSI	Nationwide Suspicious Activity Reporting Initiative
NSI PMO	Nationwide SAR Initiative Program Management Office
OS	operating system
PA	public address
PAR	Personnel Accountability Report
PCR	patient care report
PDA	Personal Digital Assistant
PIP	point in polygon
PJL	Printer Job Language [Hewlett-Packard]
PRF	Policy Routing Function
PSAP	Public Safety Answering Point
PSDI	Public Safety Data Interoperability
PTS	patient tracking systems
QA	Quality Assurance
QoS	Quality of Service
RCL	road center line
RFI	Request for Information
RFP	Request for Proposals
RMS	Records Management Systems
SAR	Suspicious Activity Reporting
SIF	Spatial Information Function
SIP	Session Initiated Protocol
SMS	Short Message Service
SOA	Service-Oriented Architecture
SOP	Standard Operating Procedure
SSM	System Status Management
SSP	Global Service Specification Packages
SWAT	Special Weapons and Tactics
tac	tactical
TMD	Tactical Map Display
TSP	Telematics Service Provider
UCAD	Unified CAD
UCADFR	Unified CAD Functional Requirements

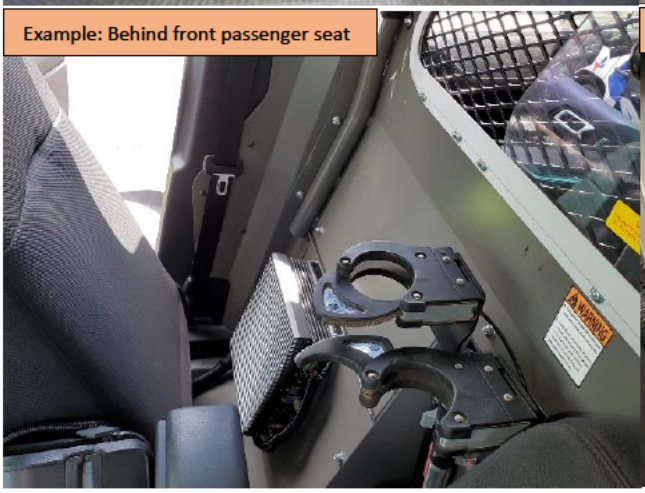
ACRONYM OR ABBREVIATION	DEFINITION
UCR	Uniform Crime Reports
UPC	universal product code
UPS	uninterrupted power system
USAR	Urban Search and Rescue
VoIP	Voice over Internet Protocol
WMD	Weapons of Mass Destruction
WPH1	Wireless Phase I
WPH2	Wireless Phase II
XML	eXtensible Markup Language

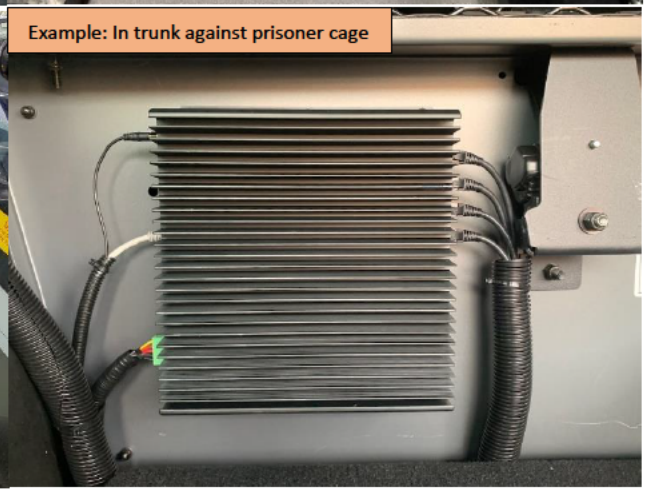
Vigilant Mobile ALPR – Installation Guide

1. Mount the VLP (Vigilant LPR Processor) where the connections will be protected from damage.

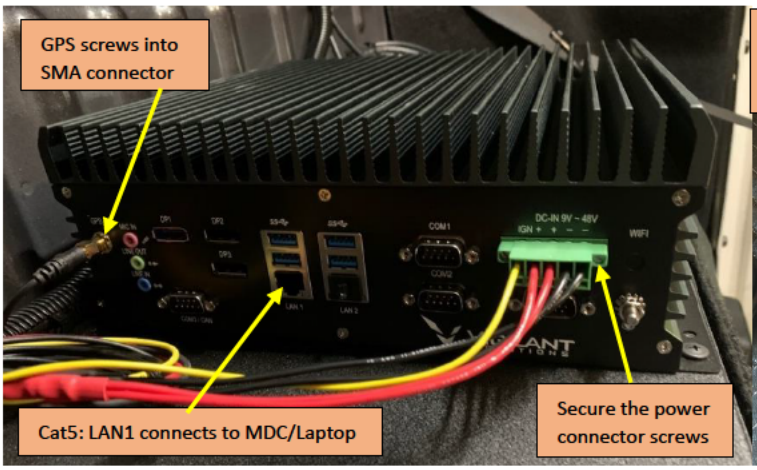








2. VLP Wiring:
   a. **Power**: Red = Constant Battery (**Important:** NO charge guards or timers, must be <u>constant</u> 12VDC)
      Yellow = Ignition (**Important:** NO timers - Must immediately turn on/off with ignition)
      Black = Ground
      NOTE: The above applies to all gas and electric/hybrid vehicles.
   b. **Cat5:** Network cable runs from LAN1 to the MDC/Laptop or docking station. The end customer may opt to plug into a local router/modem instead of the PC/docking station.



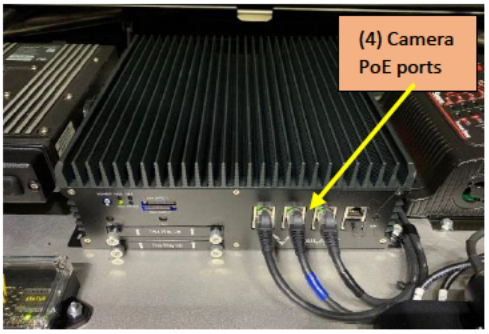


c. **GPS:** Typically mounts on dashboard using dual lock or directly on metal (bottom of GPS is magnetized).



d. **Cameras**: The cameras can be plugged into any port, but best practice is to order them as follows:

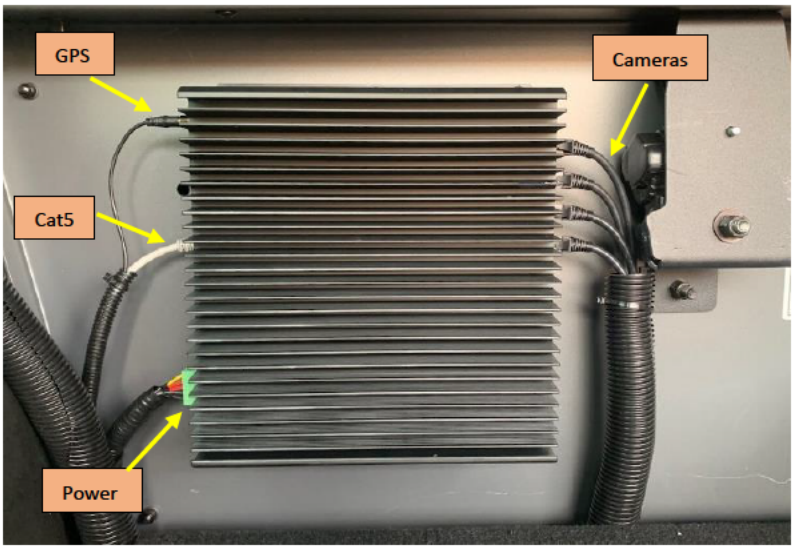
Camera 1	Front Driver
Camera 2	Front Passenger
Camera 3	Rear Passenger
Camera 4	Rear Driver





Always use dielectric grease on older Reaper HD and SD camera connectors for both new installs and RMA replacements. The Ranger L5M cameras do not require grease.

3. Completed VLP wiring:

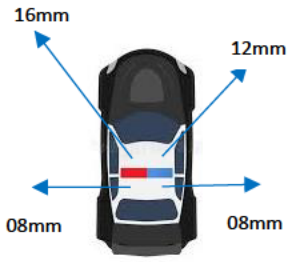


4. Camera placement: The last two numbers on the camera part label is the millimeter of the camera. Each camera type serves a specific purpose. **Contact your Customer Success Manager for questions on camera placement for each vehicle.**

Ranger L5M Part #	Reaper HD Part #	Reaper SD Part #	Focal Length	Typical Position – Use (each system will vary)
609**25**	429**25**/409**25**	209**75**	60 feet	Front Bumper - Highway Interdiction or rear facing
609**16**	429**16**/409**16**	209**35**	32 feet	Driver Front 20° - Traffic
609**12**	429**12**/409**12**	209**25**	24 feet	Passenger Front 30° – Traffic & Parallel/Angled Parking
609**08**	429**08**/409**08**	-	16 feet	Rear 90° Facing – Parking Lots/Angled Parking
609**06**	429**06**/429**06**	209**16**	12 feet	Rear 90° Facing – Parking Enforcement

Example Configurations:

City Patrol:



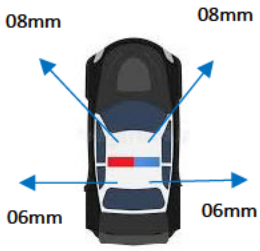
Highway Interdiction:



Urban Two-Lane:



Parking Enforcement:



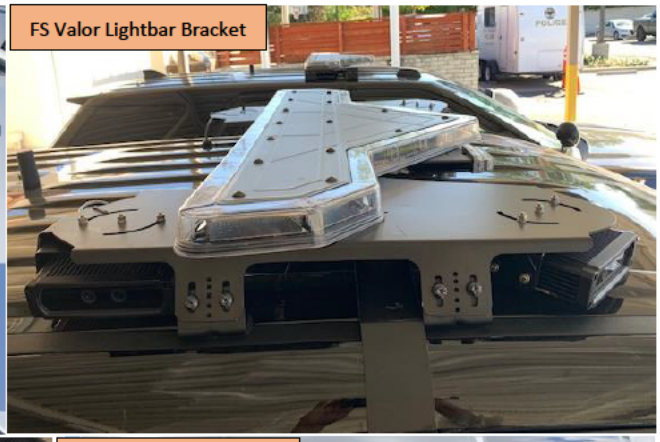
5. Camera bracket installation:

Bracket types:

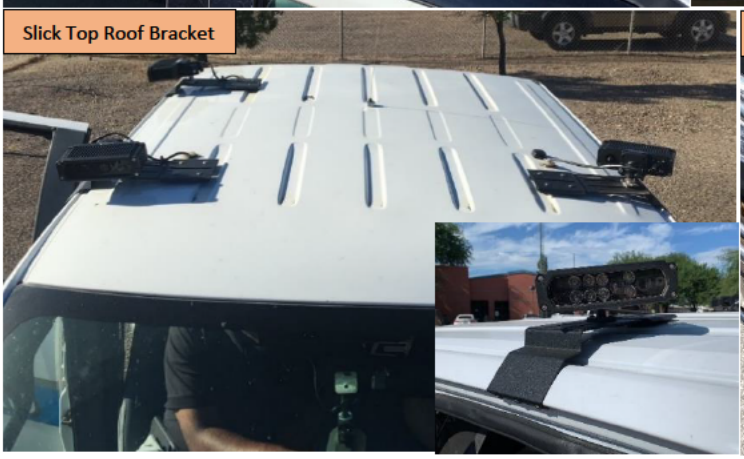
Universal Lightbar Bracket



FS Valor Lightbar Bracket



Slick Top Roof Bracket

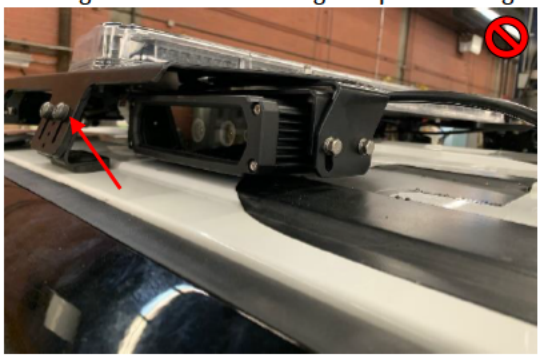


Ball Mount Bracket



Installation best practices:

- Raise lightbar feet to their highest position to give the rear cameras room to angle downward.




- Place cameras near the edge of the roof. The roof will block the camera view if they are placed too far inboard.




- Wedge the lightbar bracket between the lightbar and the lightbar foot so the cameras are near the edge of the roof.

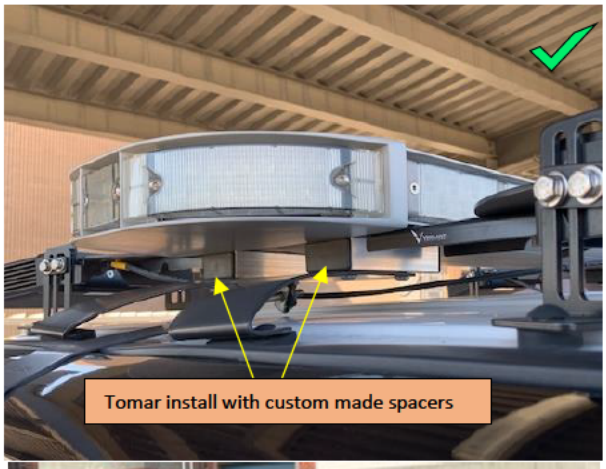



- Avoid obstructions that will block the camera view or limit the angle adjustment of the cameras.




- If needed, use the included spacers, or make custom spacers to give the cameras height above the roof, especially with low profile feet. Spacers are usually needed if the rear cameras can't achieve a downward angle of 30°.





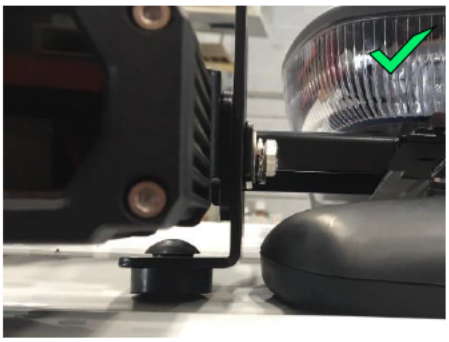




- Use appropriate sized stabilizers (long and short included) and orient them to avoid obstructions.







- Leave enough cable slack for the cameras to move freely left and right for angle adjustment.



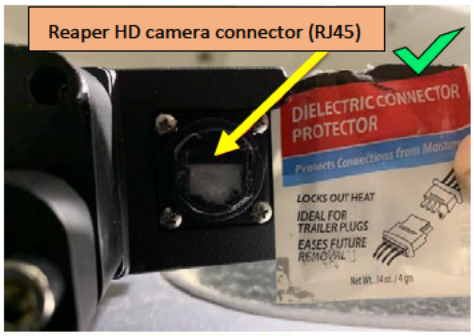


- Install cameras right side up whenever possible (Logo on the top/Serial Number on the bottom). Ranger L5M and Reaper HD cameras CAN be mounted upside down if needed. Reaper SD cameras must always be right side up.

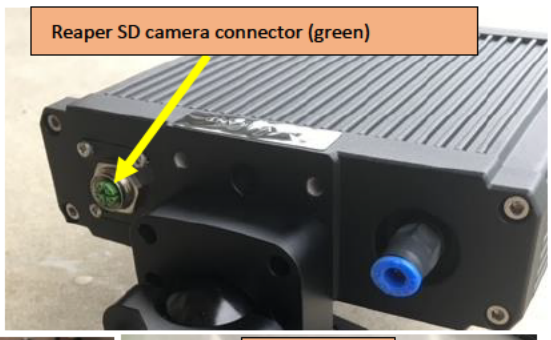




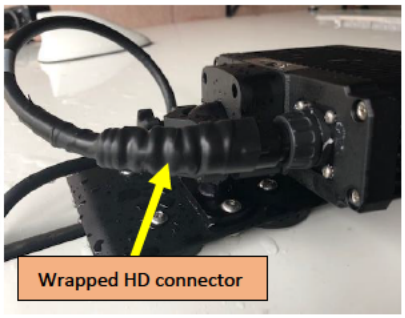
- Always use dielectric grease in Reaper HD and SD camera connectors to prevent corrosion. As an additional level of protection, you can also wrap the connector with Rubber Splicing Tape. **Ranger L5M cameras do not require grease.**

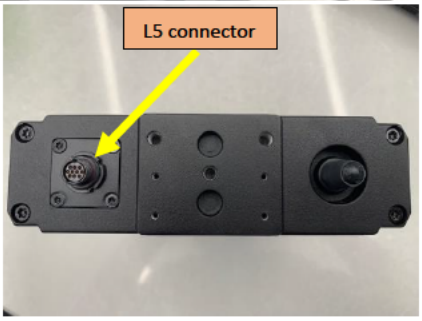




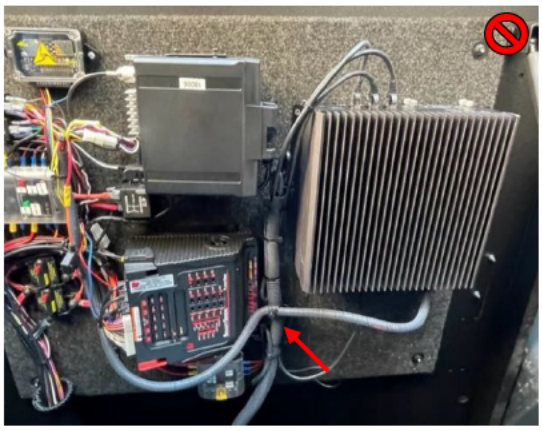


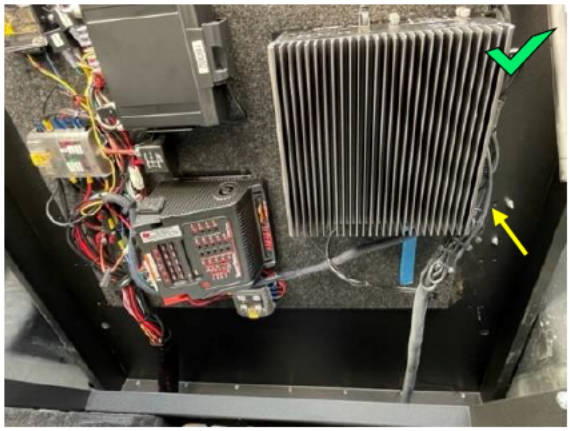






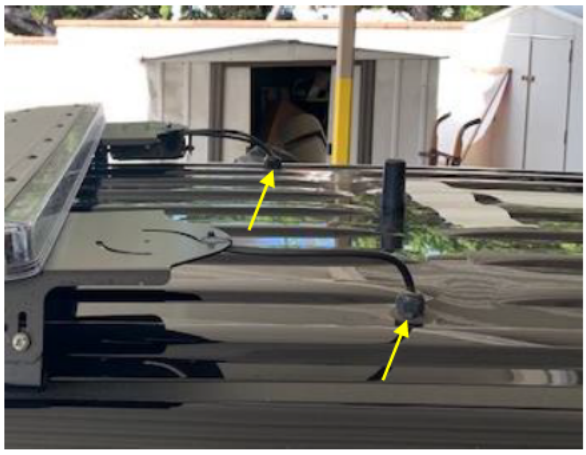
- Route camera cables away from radio equipment to avoid RF interference.





- Always use grommets and sealant in roof holes. Avoid using silicon only to fill roof holes.





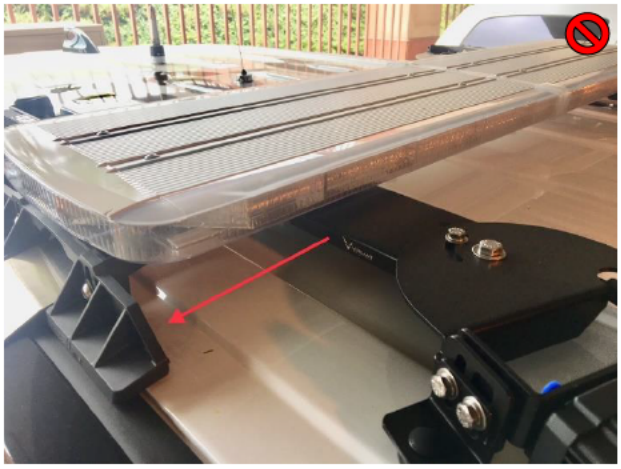
- Avoid running cables through doors and trunks where the cables can be kinked or damaged

- **NEVER open or disassemble a camera**. The cameras are nitrogen purged. Opening a camera will void the warranty.

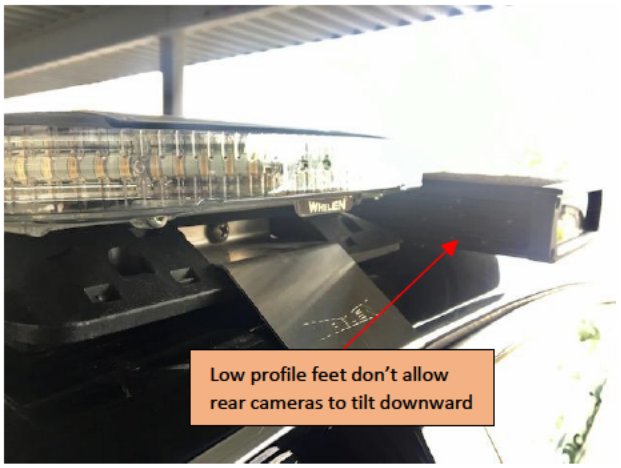
6. Bracket Specific Photos and Best Practices:

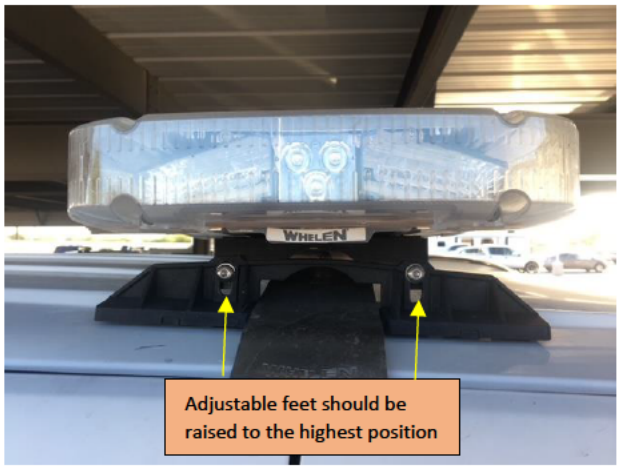
Whelen – Universal LBB:

- Whelen Lightbar: The Universal LBB should be wedged between the foot and the lightbar.
- Low profile feet should be exchanged for adjustable feet or custom spacers would need to be added.
- The installation is easier with adjustable feet but can be installed on standard feet with modifications (below):









- Typical Whelen install process:









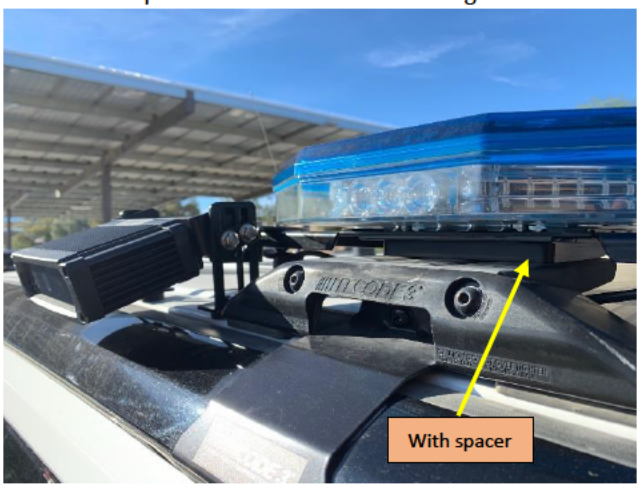




Code3 – Universal LBB:

- The Universal LBB installs easily on a Code3 Lightbar. Use the included spacer if the cameras need height off the roof:







SoundOff – Universal LBB:

- Requires drilling holes in the plastic spacer to match bolt pattern and replacing the stock 1/4-20 carriage bolts with longer 2-inch bolts.

- Typical SoundOff install process:

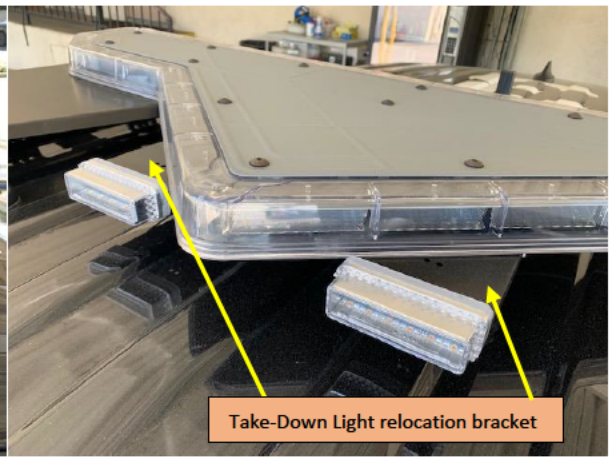


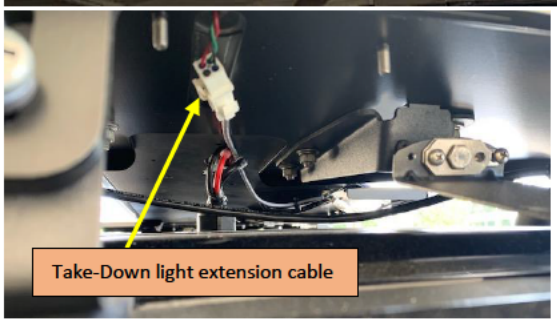
- SoundOff completed install:




Federal Signal Valor – FS-VBAR-LBB:

- The FS Valor LBB is a direct bolt in replacement for the stock lightbar feet. These brackets will also work on the older FS Vision bar with some modification to accommodate the different hole patterns.
- For Take-Down lights, use the TD relocation kit (bracket and cables) to move them to the front tip of the lightbar.



- Always install the individual camera brackets over the top of each camera (serial number label should be on bottom).




Slick Top Roof Brackets:

- Slick top mounts are designed for specific vehicles or vehicle types and screw into the door jamb like a lightbar strap and have four strong magnet feet to secure it to the roof (no holes in roof required for bracket mounting).
- Slick top mounts can be installed on vehicles with or without a lightbar.
- Forward facing cameras should mount as far forward as possible so the camera can clear the front slope of the roof
- Rear facing cameras may need to be placed near the rear of the vehicle so the view is not obstructed by the roof



- Lip Mount brackets: Lip mount brackets secure to the trunk lip using magnet feet and tension screws on the lip.



Parking Enforcement – Flat Cam Bracket

- There is not a vehicle specific bracket available for all vehicle models. The flat cam bracket is a generic bolt on bracket.
- Forward facing cameras should mount as far forward as possible so the camera can clear the front slope of the roof
- Side facing cameras should mount as close to the edge of the roof as possible to be able to angle downward
- Rear facing cameras may need to be placed near the rear of the vehicle so the view is not obstructed by the roof



Push Bar / Front Bumper Mount:

- Push Bar Mounting utilizes simple ball mount brackets:



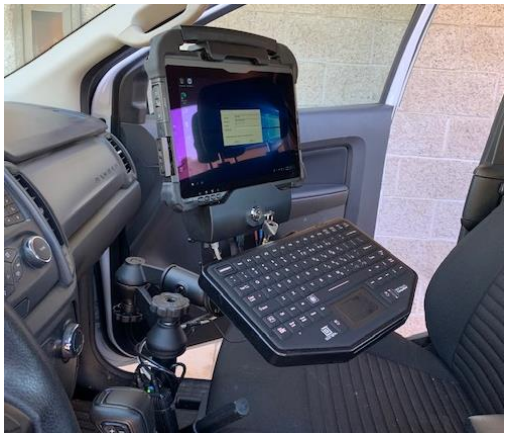
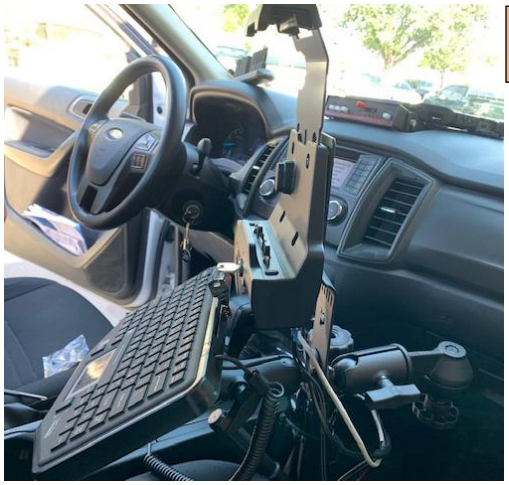





Parking Enforcement Tablet and Docking Station:

- The Parking Enforcement Tablet and docking station utilizes a No-Drill Universal Laptop Mount that attaches to the front passenger seat floor bolts.
- The kit includes extra parts for different types of installs. Only use what is needed for the specific vehicle.

- Example install for Vigilant LPR docking station and tablet:

No-Drill Universal Laptop Mount Kit



Covert Installation best practices:

- Covert installations will always involve some level of customized installation and/or fabrication. It's common practice to hide the front cameras in the front grill or bumper and the rear cameras either on the inside of the rear passenger cab (requires rolling down the windows) or in the bumper.
- The installation must allow for proper adjustment of the camera angles. If cutting of bumpers or front grills is involved, it's best to contact your Customer Success Manager to arrange for a Vigilant Field Service Engineer to be on site to align the camera angles BEFORE cutting into the vehicle.








- Vigilant does not offer vehicle specific brackets for covert installs. Basic ball mounts are typically provided.




- To ensure the camera angles are correct, it's best to contact your Customer Success Manager to arrange a technical discussion with a Vigilant Field Service Engineer.






UPLOAD ANYWHERE ANYTIME: IN-CAR VIDEO LTE UPLOAD GUIDE

FOR PLANNING AND IMPLEMENTING 4RE® IN-CAR AND VISTA® BODY CAMERA UPLOAD OVER CELLULAR LTE CONNECTION

WATCH GUARD

Overview

This document describes the technical requirements and implications for implementing video upload over a cellular data link in vehicles equipped with a WatchGuard 4RE in-car camera system. (If a vehicle is equipped with a VISTA WiFi body camera and WiFi base/dock, its video will be uploaded over the cellular data link as well).

The target audience for this document is WatchGuard customers who are interested in incorporating this capability into their vehicle fleet.

The objectives of this document are (1) to explain the potential benefits of uploading video over cellular data link and (2) to describe the configuration options and requirements for a successful implementation.

This document covers the main points, for the best experience we recommend a full network diagram be created for your agency's connectivity.

Benefits of Uploading Video over Cellular

If an agency meets the requirements and recommendations for uploading video over cellular, they can experience the following benefits:

- Vehicles will need to return to a central location to upload video over WiFi less frequently and for shorter durations or eliminate the need to upload over WiFi at all.
- Video evidence will be available sooner in Evidence Library, so Administrative staff can view events soon after the incident occurs without the vehicle coming back to the station.
- For take home vehicles, reduces the time to upload video from the parking lot.
- If uploading cellular only, it cuts down on necessary network infrastructure for traditional 802.11 Wireless networks.
- If utilizing FirstNet, your agency's evidence gets priority on the bandwidth.

Potential Downsides

Potential downsides of implementing video upload over cellular data link include:

- The cost of equipping vehicles with cellular routers or cellular data link service may be prohibitive to some agencies.
- The additional load on vehicle systems may be unacceptable. This includes the total usage of the cellular data link as well as possible additional loading on the Mobile Data Computer and its data link. (Note: PC applications can be used on an MDC to manage the processing load and cellular data link usage and potentially resolve any issues related to the additional load).

- The cellular service provider may throttle cellular data when some threshold is reached (i.e. after uploading 50 GB of data for a given pay period, the upload speeds drop from 10 Mbps to 0.5 Mbps). The addition of video uploading onto the data link will cause throttling to occur more often/sooner.

Key Points

Here are the key messages addressed in this document.

1. **Cellular upload of video is entirely dependent on the bandwidth provided by the desired cellular service provider across a geographical region.** This bandwidth can vary widely and, in some cases, may not be sufficient to provide significant benefits.
2. There are many possible vehicle configurations to support video upload over cellular data link, but **only a specific set of configurations that have been validated and are supported by WatchGuard.** Configurations other than those recommended will require testing and verifying in the field by your agency and may have ongoing technical obstacles to overcome in order to have a viable implementation.
3. If your agency has **vehicles outfitted with an Ubiquiti Bullet (shown below) WiFi radio**, you must either:
    a. Use a cellular router which provides both WiFi and cellular data links (such as the cellular routers recommended in this document) or



    b. Replace the Ubiquiti Bullet radio with a MikroTik Groove radio to upload video via WiFi, incorporation with an MDC/Laptop with cellular connection
4. **Re-configuration of the cellular router** may be required to utilize both cellular and WiFi data links (setup is required for WiFi path and priority/switching).

Requirements

1. 4RE in car system with the following items:
    a. Smart Power Switch (SPS)
    b. 4RE firmware version 4.0.7 or higher
    c. Run WatchGuard provided scripts on 4RE via USB drive
    d. Optional: VISTA WiFi docking base if uploading video
2. Cellular device via one of the following device types:
    a. Mobile gateway device (examples: Sierra Wireless, CradlePoint)
    b. Laptop/MDC with an Internet connection via MiFi or embedded SIM card – will require PowerShell scripts to run on laptop (Windows 10 recommended)
3. Cellular SIM and data plan: WatchGuard recommends purchasing a plan that will not throttle speeds
4. Evidence Library Configuration:

a. If using On-Premise Evidence Library –
    i. Evidence Library 4.2 or higher
    ii. Option 1 – Encrypted upload over the Internet:
        1. Provide a public **static** public IP address or public DNS Name and open TCP ports: 5002 and 9145
        2. Install and configure stunnel
    iii. Option 2: Encrypted over a VPN to Evidence Library Server
        1. VPN client on cellular modem or MDC
        2. VPN on Evidence Library Server

b. If using EvidenceLibrary.com (Cloud Hosted Solution)
    i. Option 1: WatchGuard will host an upload server in the Azure Government cloud and configure stunnel (may be additional cost)
    ii. Option 2 - Encrypted upload over the Internet
        1. Provide a public static or public DNS and open TCP ports: 5002 and 9145 for the upload appliance
        2. Install and config stunnel
    iii. Option 3: Encrypted over a VPN to Upload Appliance
        1. VPN client on cellular modem or MDC
        2. VPN client Upload Appliance
        3. VPN connection to the Evidence Library Server

Caveat: VISTA WiFi “cellular upload” is not an option with the **On-Premise** of Evidence Library configuration until version 5.1 (ETA: Summer 2019).

Is Your Agency a Good Candidate for Cellular Upload of Video?

There are numerous variables involved when implementing a cellular upload capability into your vehicle fleet. Among these variables are things like type of cellular router/modem, cellular service provider, cellular service type, cellular service geographical variations, agency security requirements, and agency policies.

This document is intended to help your agency understand the potential benefits of implementing video upload over cellular data link as well as any associated risks or difficulties you may encounter. This will enable to your agency to make an informed decision about how to proceed with this capability.

Here is a high-level overview of what makes a good candidate for implementing video upload over cellular data link.

An Agency is a Good Candidate if:

- It understands the technical limitations of uploading video over cellular as explained in this document.
- It uses one of the WatchGuard supported cellular routers or one of the WatchGuard supported MDC/cellular modem combinations.

- It uses the WatchGuard recommended system configuration (as described in this document).
- Its cellular service provider has good upload speeds and signal coverage over the agency's geographical service area.
- Its policies are supportive of uploading video over cellular data link.

An Agency is a Potential Candidate if:

- It uses a configuration other than the WatchGuard recommended configuration but is willing to do some testing and experimentation to determine whether their configuration will support video upload over cellular in a satisfactory manner.

An Agency is Not a Good Candidate if:

- It has overly optimistic expectations for the performance of video upload over cellular which are beyond the technical limitations of the system. (This document is intended to help avoid this situation).
- It uses a configuration other than the WatchGuard recommended configuration and is unable to achieve satisfactory performance from this configuration.
- Its cellular service provider has poor upload speeds and signal coverage over the agency's geographical service area. Use speedtest.net or other speed tests in multiple areas in your area of patrol to confirm speeds.
- Its policies are not supportive of uploading video over cellular data link.

Estimating Potential Improvements in Video Upload

Given the many variables involved, it is not possible to accurately predict the performance gains that may be experienced by implementing video upload over cellular. To fully determine actual system performance, technical measurements must be made in the field under live operational conditions.

The **most significant determiner** of how much video can be offloaded using the cellular data link is the **available bandwidth from the cellular service provider**. This bandwidth can vary widely across a geographical region and is independent of signal strength (bandwidth may be low even when signal is strong). When the upload bandwidth is consistently ample (say 15Mbps or higher) across a service area, it is possible for most or all of a vehicle's recorded video to be uploaded using only the cellular data link. However, the upload bandwidth is often much lower and can vary widely across the service area to a point where little or no video may be uploaded in a given time.

Here are some online tools to see cellular providers and their coverage with 3G or 4G:
https://www.whistleout.com/CellPhones/Guides/Coverage

4G/LTE or 3G?

Is 3G enough, or does your agency need 4G/LTE?

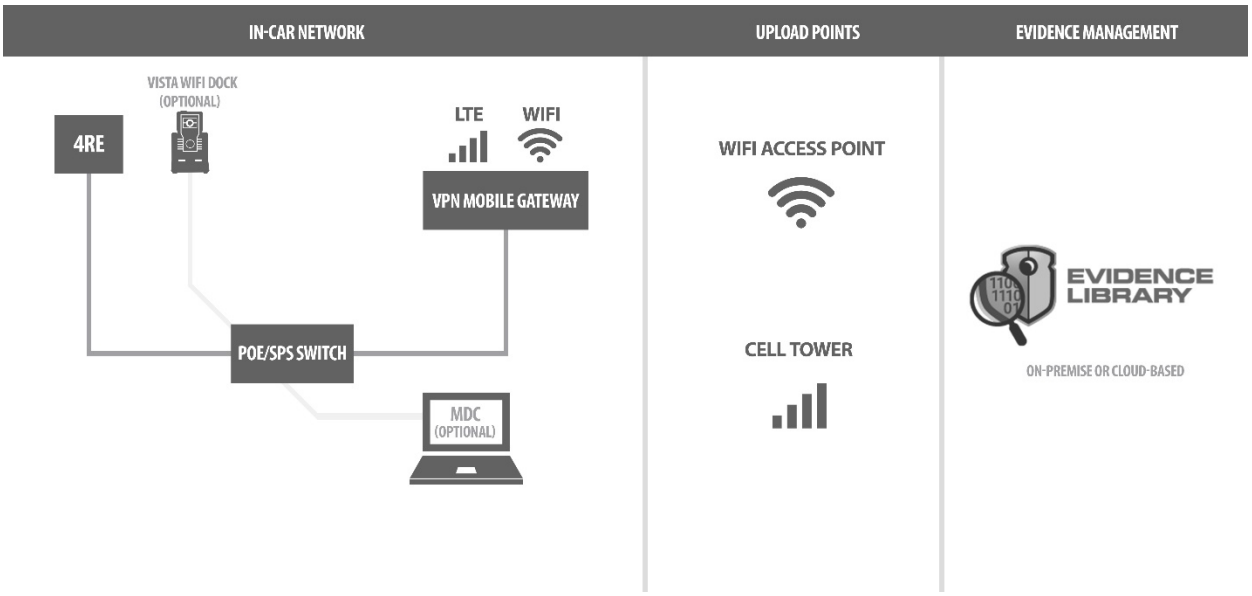
The faster speeds are better, as it gets the video uploaded and viewable faster. 3G **theoretical** maximum speeds are about 21 Mbps. With a moving vehicle, those speeds are drastically decreased (sometimes down to 300 Kbps). On average, WatchGuard has seen between 300Kbps and 3 Mbps with a 3G connection. Each provider will be different. The 4RE in-car system or VISTA body camera can upload with those speeds between 1 and 3 Mbps. However, the amount of data created will need to be **monitored closely**. WatchGuard recommends that a WiFi connection is also used in this configuration to allow upload to finish in a WiFi hotspot area.

FirstNet is another tool to help with uploading video. If utilizing a FirstNet SIM card, the upload speeds can be more consistent. The WatchGuard system is compatible with FirstNet.

Recommended Configurations

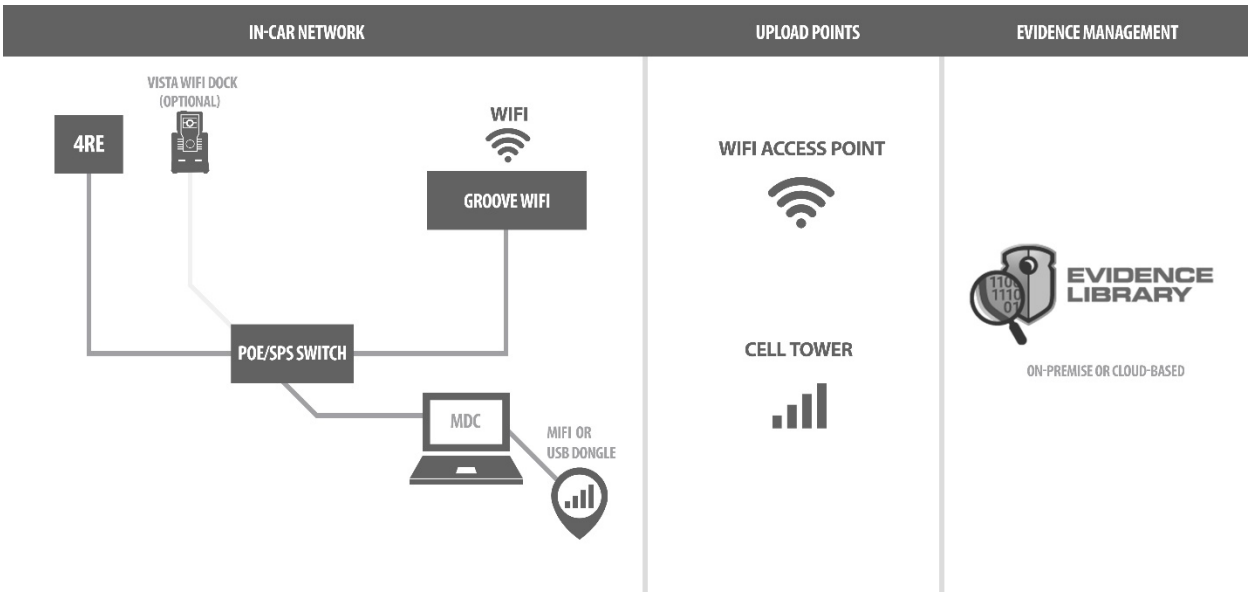
There are two main system configurations to support video upload over cellular data link. The physical components are similar, but there are different ways to implement this configuration.

The first configuration uses a mobile gateway or dedicated modem with Ethernet ports. This option is desirable for customers who are looking to add mobile gateway devices (e.g. Sierra Wireless MP70, MG90, Cradle Point IBR900) or already have a similar device. The 4RE in-car system would connect via Ethernet to that device. The mobile gateway would try to connect via WiFi first, and if it isn't available, connect to the cellular tower instead for uploading video. Then it would upload to the backend video management system Evidence Library.



The second configuration uses the MDC with a USB dongle, embedded SIM card, or “MiFi” device. The second configuration is desirable for agencies with a low budget for cellular upload and would like to keep the in-car hardware the same or with a minimal change.

The 4RE in-car system would be configured to connect to the MikroTik Groove client for upload via WiFi and the laptop for cellular upload. The system is configured to connect to agency’s WiFi access point via MikroTik WiFi radio, and if WiFi isn’t available, then connect to the cellular tower via the MiFi or other cellular connection for uploading video. Then it would upload to the backend video management system Evidence Library.



Encryption Configurations

Since most of the video uploading is evidence, the system is designed to upload the video with encryption. The encryption can be done by two different methods:

Method 1:

- Stunnel as the encryption method. WatchGuard would install and configure this option.
    - A FIPS 140-2 compliant application to encrypt upload traffic.
- WatchGuard Technical Services can help on the implementation plan.

Method 2:

- Utilize a VPN for the encryption method.
- The VPN client would be installed on the mobile gateway device or on the MDC laptop.

Questions?

Contact us to see if cellular upload technology is right for you.

(800) 605-6734
watchguardvideo.com

VEHICLE INSTALLATION INSTRUCTIONS



USER GUIDE

Important Notice

Copyright © 2020 WatchGuard, Inc. All rights reserved. This document and supporting data are the exclusive property of WatchGuard, Inc. and may not be copied and/or reproduced without permission.

Software and firmware updates

WatchGuard is committed to the continual testing and improvement of our software and firmware. As new revisions become available, these updates will be made available to your agency. Fees may apply depending on your licensing agreement.

Contact information

WatchGuard, Inc.

415 East Exchange Parkway

Allen, Texas 75002

Customer Service: 800-605-6734

Customer Service web portal: **https://support.watchguardvideo.com/hc/en-us**

Send us your suggestions

Tell us about your experience and how you are using WatchGuard products. We will do our best to accommodate any suggestions you may have in future products.

U.S. customers, call Customer Service or submit a ticket through the Customer Service web portal. International customers, contact your local distributor or submit a ticket through the Customer Service web portal.

Trademark notices

3M, Scotch, and Super 33+ are worldwide trademarks or registered trademarks of 3M.

Cradlepoint and IBR900 are trademarks of Cradlepoint, Inc. in the US and other countries.

MikroTik is a registered trademark of SIA Mikrotikls.

Sierra Wireless® and AirLink® are registered trademarks of Sierra Wireless.

Ubiquiti® and Bullet™ are trademarks or registered trademarks of Ubiquiti Networks, Inc., in the United States and in other countries.

VELCRO® is a registered trademark of Velcro Industries B. V.

Wi-Fi® is a registered trademark of Wi-Fi Alliance.

All other marks, names, and logos are the property of their respective owners.

Contents

Introduction **5**
About this document 5
Related documents and information 6
Installation training 6
Preparing for the Installation **7**
Overview 8
Before Installing the System in a Vehicle 9
Standard Parts Lists 10
4RE standard parts list 10
VISTA WiFi or VISTA XLT standard parts list 11
V300 standard parts list 12
Recommended Tools 13
Installation Required Practices 14
Cables 14
HDMI cables 14
Pulling cables 14
Cameras 15
Connections 15
HiFi Microphone antenna 15
Power 15
Wireless radio 15
Installing the System **17**
Overview 18
Recommended Installation Workflow 19
Installing Cameras in the 4RE System 23
Installing the front camera using the puck 23
Panoramic X2 HD 25
Zero Sightline 25
HD Mini Zoom 26
Installing the cabin and other secondary cameras 26

Contents

Notes for secondary camera installation 27
Installing the 4RE DVR Display 28
Installing the 4RE DVR 29
Installing a PoE adapter 31
Installing a PoE Switch 33
Installing the Wireless Radio 35
Mounting the wireless radio antenna 36
MikroTik Groove 39
Installing the 4RE/VISTA or 4RE/V300 System 40
Installing the Smart Power Switch 41
Installing the Smart Power Switch power cable 42
Installing the VISTA or V300 WiFi Base 44
Installing Microphones in the System 45
Installing the HiFi Microphone 45
Installing the cabin microphone 46
Installing the GPS Antenna 47
Connecting the External Inputs Cable 48
Connecting the System Power Cable to the Vehicle Battery 50
Testing the System Installation 52
Appendix A: Cellular LTE Upload 55
Appendix B: WatchGuard Mobile LPR 56
Index 57

Introduction

Welcome to the WatchGuard *4RE Vehicle Installation Instructions*. This guide is designed to provide basic information and instructions for installing the WatchGuard 4RE DVR and the VISTA or V300 body camera, with their related components, in a vehicle.

About this document

The *4RE Vehicle Installation Instructions* covers the following topics:

- Preparing for a vehicle installation, including:
  - Pre-install checklist
  - Example installation parts lists and recommended tools
  - Installation best practices
- Installing WatchGuard equipment in a vehicle, including:
  - Recommended installation workflow
  - Cameras
  - 4RE DVR
  - VISTA and VISTA WiFi Base or V300 and V300 WiFi Base
  - Wireless radio
  - Microphones
  - Related components and cables
- Testing the installation

This document also includes appendices that list basic equipment that can be added to a 4RE vehicle installation to provide additional functionality:

- Appendix A: Cellular LTE Upload
- Appendix B: WatchGuard Mobile LPR

The images in this document are representative of what you could experience while installing. They are meant to serve as a guide.

This guide contains general recommended instructions for installing a WatchGuard system in a vehicle. This document is not an exclusive or comprehensive blueprint for any particular vehicle installation. If you have a question about installing the system in a particular vehicle, contact WatchGuard Customer Service.



Important! *This document assumes knowledge of standard 12-volt vehicle installation best practices. It is meant to guide a technician through the specifics of installing WatchGuard equipment.*

Related documents and information

For further information related to installing WatchGuard equipment in a vehicle that is not covered by the *4RE Vehicle Installation Instructions*, see the following documents:

- *4RE Installation Poster*
- *WatchGuard Bracket Guides*
- *4RE In-Car DVR User Guide*
- *VISTA HD Wearable Camera User Guide*
- *V300 Quick Start Guide*
- *Evidence Library Online Help*
- *HiFi Microphone User Guide*

Installation training

WatchGuard offers factory training courses several times per year for installers to become certified in WatchGuard equipment installation. For more information and to register, go to **http://watchguardvideo.com/training**.

Preparing for the Installation

In this section...

- Pre-installation checklist (**page 9**)
- Standard installation parts list examples (**page 10**)
- Recommended tools list (**page 13**)
- Installation required practices (**page 14**)

Overview

This section includes information to help you prepare for the in-vehicle installation of the WatchGuard 4RE DVR and the VISTA or V300 body camera and their related components. The section includes:

- **Pre-installation checklist**: Complete the items on this checklist before starting the installation (page 9)
- **Standard installation parts lists**: Contains examples of parts lists for standard 4RE/VISTA or 4RE/V300 vehicle installations (page 10)
- **Recommended tools list**: Shows a list of tools, including some specialized items, you should have at hand before beginning the installation (page 13)
- **Installation required practices**: Lists a number of best practices that WatchGuard requires you to follow as you perform the vehicle installation (page 14)

Before Installing the System in a Vehicle

Use the following list to help you prepare for a successful 4RE/VISTA or 4RE/V300 system installation in a vehicle:

- Prepare to document the installation for a first-time vehicle (year and/or model), as applicable
- Gather all necessary tools for the installation (page 13)
- Remove any old video equipment, as applicable
- Verify that you have received all the components for the 4RE/VISTA or 4RE/V300 system that you are installing (page 10)

  Note: *If you have any missing or damaged parts, contact WatchGuard Customer Service.*

  - Make sure the mounting brackets are the correct type for the specific vehicle

    Note: *When installing brackets, follow the instructions included with the bracket. If you need a copy of the bracket instructions, contact WatchGuard Customer Service.*

- Determine the installation locations (installation plan) for all components (including brackets and cables)
  - Determine the wire connection points, for example, vehicle battery location, emergency light input, brake input, auxiliary input
- Roughly lay out the main components in their installation locations to test positioning
- Read through the *Installation Required Practices* (page 14) and add them to your installation plan

Tip: *Use the 4RE installation overview poster as a reference for the installation. You can download a copy of the installation poster from the WatchGuard Video website:* ***https://support.watchguardvideo.com/hc/en-us***

Standard Parts Lists

The parts lists in this section are included as examples. Your installation equipment order includes the actual parts list for your installation.

If you need additional parts, contact WatchGuard Customer Service.

4RE standard parts list

The following table lists the standard parts included for a 4RE system installation (with wireless upload) in a vehicle.

Qty	Part Number	Description
1	WGA00428-101	MikroTik Configured Wireless Kit, 4RE In-Car 802.11n (Radio, Antenna, PoE, 2-10' Ethernet Cables)
1	WGP01394-001	Cable, WiFi Vehicle Antenna Mount, NMO, Drill 3/4" Hole, 17' long
1	WGA00480-101	4RE, HD DVR, Gen 2, 200GB HDD
1	WGA00370-200	4RE, Remote Display Control Panel, Gen 3
1	WGA00496	Front Camera, 4RE, HD Zero Sightline (ZSL)
Or 1	WGA00543	Front Camera, 4RE, HD Panoramic
Or 1	WGA00500	Front Camera, 4RE, HD Mini Zoom
1	WGP01760-200	Camera, Infrared Analog, WMv.2, 114 Degree, 2-Pin Connector
1	WGP01903-001	Cable, 4RE, HDMI, (HD Mini Zoom, Panoramic, ZSL) Straight, 15'
1	WGP01832	Cable, 4RE, HDMI, Port 2 IR Camera, 2-Pin Connect, Straight, 16' (5000mm)
1	WGP02055-KIT	R/A Adapter KIT, HDMI Cables, Dual Mount Bracket, 4RE DVR
1	WGA00382-100	Cable, 4RE, HDMI/Mini, Display ONLY, Straight, 15'
1	WGA00420	Bracket Kit, 4RE, Display, w/ Diamond 1" Ball Mounts & 2" RAM
1	WGP01459-008-KIT	Bracket Kit, 4RE, Display, Universal Visor Post (Ford PI SUV & Sedan)
1	WGP01443-001-KIT	Bracket Kit, 4RE, DVR, Universal

Qty	Part Number	Description
1	WGP01487-KIT	Bracket Kit, 4RE, DVR, Console Faceplate, 2"
1	WGP362	GPS Antenna, Magnetic Mount
1	WGP02073-300-KIT	Cable Assembly, DV-1C/4RE, Power/Input, R/A 24'
1	WGA00475-KIT1-V2	Hi-Fi Microphone Kit 1v.2 (Transmitter, Cradle, Belt clip, Pivot clip, 3' + 12' antenna)
1	WGP01475	Bracket, Hi-Fi Microphone, Universal
1	WGA00510-005	Cable Assembly, DVR to Hi-Fi MIC, 180"
1	WGP412	Cabin Microphone - 7'
1	WGP412-300	Cabin Microphone Extension Cable - 12'
1	WGD00085-KIT	Kit, 4RE DVR Installation Kit
1	WGD00089-KIT	Kit, 4RE In-Car Video System User Guide
1	WGD00122	Document, Groove Setup Instructions

VISTA WiFi or VISTA XLT standard parts list

The following table lists the standard parts included when adding integrated VISTA WiFi or VISTA XLT body camera to the 4RE system installation in a vehicle.

Qty	Part Number	Description
1	WGA00600	VISTA HD, WiFi Extended Wearable Camera
OR		
1	VIS-XLT-WIF-001	VISTA XLT Wi-Fi System Body-Mounted Camera Kit
OR		
1	VIS-XLT-WIF-002	VISTA XLT Wi-Fi System Head-Mounted Camera Kit
1	WGA00586-KIT	VISTA HD, WiFi Charging Radio Base Kit, incl. Power and Cables
1	WGA00574	4RE, VISTA HD WiFi, Smart PoE Switch
1	WGP02225-203-KIT	Bracket, VISTA WiFi base Universal, All-In-One, with Screws
1	WGP02225-202-KIT	Bracket Kit, Wi-Fi Base, Universal w/ screws

V300 standard parts list

The following table lists the standard parts included when adding the V300 body camera to the 4RE system installation in a vehicle.

Qty	Part Number	Description
1	WGA00625	V300 Wearable Camera
1	WGA00635-KIT	V300 WiFi Dock, D330, In-Vehicle Charge/Upload Kit, incl. Cables and Brackets
1	WGA00635	V300 Base Assembly, WiFi Dock
1	WGP02494	Cable Assembly, Bullet to Antenna, Smart POE Switch
1	WGP02495	Cable Assembly, Power, Smart POE Switch
1	WGP02791	Cable Assembly, RJ50 10P10C, Straight, 25FT, G2 Wear, WiFi Base
1	WGP01090-001	Cable Assembly, Straight Ethernet, CAT5E, 5FT
1	WGP584-102	Cable Assembly, Fused, +12V, 7.5 AMP
1	WGP587-103	Cable Assembly, Battery Ground 16 AWG, 16IN
1	WGP582-002	Fuse, ATO/ATC, 7.5 AMP
1	WGP02504	Antenna, Windshield Mount, 2.4 GHz, 3FT, VISTA WiFi Base
1	WGP01573-400	Extension Cable, PFP195, 12FT, PCTEL WiFi Antenna to VISTA WiFi Base
1	WGP02225-202-KIT	Bracket Kit, WiFi Base, Universal, w/ Screws
1	WGP02225-203-KIT	Bracket Kit, WiFi Base, Offset, w/ Screws

Recommended Tools

The following tools are recommended for installing the 4RE DVR and VISTA or V300 body camera and their related components in a vehicle.

- Drill and bits, including 3/4-inch bit for antenna mounting
- Coarse sandpaper, 60 or 80 grain
- 10-30 feet of 16-20 gauge primary wire for extending input cable connections if necessary
- Wire strippers
- Wire crimpers
- Various wrenches and sockets, including 24mm or 15/16-inch open-ended wrench
- Pliers
- Utility knife
- Torx® screwdrivers or bits, sizes T20, T15, and T10
- 1/16-inch hex screwdriver or Allen® wrench
- Electrical tape and/or heat-shrink tubing
- Zip ties
- Hand-held butane torch or lighter (Optional)
- Loctite® 312 adhesive and primer
- 3M™ Scotch® Super 33+™ tape

Installation Required Practices

Important! *These practices are required by WatchGuard. Using them helps you have a more successful installation experience.*

Cables

HDMI cables

Important! *The HDMI cables included with the WatchGuard installation kits are customized to be as rugged as possible; however, HDMI cables are very susceptible to damage. They do not work if kinked or pinched.*

Keep the following required practices in mind when working with the system HDMI cables:

- Be careful of cable bends—use no more than a soft S-bend
- Leave the plastic caps on the cable ends until you are ready to connect them to a component
- Use the 10 VELCRO® strips included with each system when you install the HDMI cables
- If you use zip ties on HDMI cables, make the loops loose enough to allow the cable or cable bundle to barely spin in the loop

  Zip ties that are pulled too tight damage HDMI cables. Be careful not to damage the HDMI cables if you use a zip tie gun.

Tip: *If you are mounting the 4RE DVR in the console, you may need to use the HDMI right-angle adapter kit to avoid making sharp bends in the HDMI cables where they connect to the 4RE DVR. For more information and to order the kit, contact WatchGuard Customer Service.*

Pulling cables

Pulling cables in the vehicle can be difficult and can damage the cables. Order and install new cables if you move a system from one vehicle to another.

Cameras

If you plan to mount the front camera on a puck, install the puck on the windshield first to allow the glue to dry.

Tip: *You can use a hand-held butane torch or lighter to heat the puck. This can help speed up the installation process (page 23).*

Connections

- Always butt-splice and crimp wire connections

  Important! *Do not use 3M™ ScotchLok™ or similar types of connectors.*

- Use 3M Scotch® Super 33+™ tape to cover any soldered electrical connections

HiFi Microphone antenna

Always position and install the HiFi Microphone (HiFi Mic) antenna horizontally. The antenna inside the HiFi Mic transmitter is horizontal. For good performance, you should mount the HiFi Mic antenna horizontally to match.

Warning! *Do not follow the manufacturer's online specifications for installing the antenna vertically. If you mount the antenna vertically, the HiFi Mic loses 90 percent of its operational range.*

Power

Wire power to the battery. The battery is the cleanest source of power in the vehicle.

Wireless radio

Always mount the wireless radio in a position where you can easily see its LEDs. Access to the LEDs is needed for diagnostic purposes.

Important! *Do not mount the wireless radio in a location that is difficult to access, for example, in the console.*

This page intentionally left blank.

Installing the System

In this section...

- Recommended installation workflow (page 19)
- Installation information and procedures for:
  - Front and secondary cameras (page 23)
  - 4RE DVR (page 29) and its display (page 28)
  - PoE (power over Ethernet) adapter (page 31) and switch (page 33)
  - Smart Power Switch (page 41)
  - Wireless radio and its antenna (page 35)
  - Wireless and cabin microphones (page 45)
  - VISTA or V300 WiFi Base (page 44)
  - GPS antenna (page 47)
  - Connecting the system to external inputs (page 48)
  - Connecting power to the 4RE (page 50)
  - Connecting power to the Smart Power Switch (page 42)
- Testing the 4RE/VISTA or 4RE/V300 installation (page 52)

Overview

This section includes a full system installation workflow (page 19). WatchGuard recommends that you follow this workflow for best results.

It also includes individual sections for installing the following components:

- Front and secondary cameras (page 23)
- 4RE DVR (page 29) and its display (page 28)
- PoE (power over Ethernet) adapter (page 31) and switch (page 33)
- Smart Power Switch (page 41)
- Wireless radio and its antenna (page 35)
- Wireless and cabin microphones (page 45)
- VISTA or V300 WiFi Base (page 44)
- GPS antenna (page 47)
- Connecting the system to external inputs (page 48)
- Connecting power to the 4RE (page 50)
- Connecting power to the Smart Power Switch (page 42)

The final section provides instructions for testing the 4RE installation (page 52).

Recommended Installation Workflow

The following steps make up a recommended workflow for installing the 4RE DVR and the VISTA or V300 body camera with their related components:

Warning! *Only connect cables when this workflow instructs you to. Connecting cables out of sequence can damage components.*

1. Complete all items in the *Before Installing the 4RE System in a Vehicle* list (page 9).
2. Remove vehicle panels, as needed.
3. Remove cables from their packaging, and roughly lay them throughout the vehicle to verify routing and length.

   Note: *If a cable is too short, contact WatchGuard customer service for a longer cable.*

4. Install the **front camera** (page 23):
   a. **If you are using a puck (rearview mirror button)**, glue the puck to the windshield. (page 23)

      If you are using a front camera bracket, install the bracket then attach the camera to it.
   b. Connect the HDMI cable to the front camera then run it to the location where you will install the 4RE DVR, but DO NOT connect the cable to the 4RE.
5. Install the **4RE Display** (page 28):
   a. Position and install the display bracket.
   b. Install the bracket-side RAM® ball on the display bracket.
   c. On the back of the display, connect the HDMI cable.
   d. Install the display-side RAM bracket and ball on the back of the display.
   e. Attach the display to the display bracket using the RAM ball mount.
   f. Run the HDMI cable to the DVR location, but DO NOT connect it to the 4RE DVR.
6. Install the **4RE DVR** (page 29):
   a. Install the DVR bracket.
   b. Position and loosely install the DVR, but DO NOT connect cables to it.

7. Perform one of the following options, depending on the equipment you have:

   If you have a wireless radio kit, position and install (but DO NOT connect cables):

   - PoE (power over Ethernet) adapter (**page 31**) or PoE switch (**page 33**)

   > ***Note:*** *If you have a switch in your set of components to be installed, you should install the switch, not the adapter.*

   - Wireless radio (**page 35**)

   If you have a wireless radio kit AND a VISTA WiFi or V300 kit, position and install (but DO NOT connect cables):

   - Smart Power Switch (**page 41**)
   - Wireless radio (**page 35**)

   If you have a VISTA WiFi or V300 kit but NO wireless radio kit, position and install (but DO NOT connect cables):

   - Smart Power Switch (**page 41**)

   If you have a mobile data computer (MDC) kit, and/or a modem, AND a VISTA WiFi or V300 kit, position and install (but DO NOT connect cables):

   - Smart Power Switch (**page 41**)

   If you have an MDC kit, and/or a modem, but NO VISTA WiFi or V300 kit, position and install (but DO NOT connect cables):

   - PoE switch (**page 33**)

8. **If you have a wireless radio kit**, install the wireless radio antenna and the radio-to-4RE Ethernet cables:

   a. Mount (drilled, magnetic, or trunk mount) the wireless radio antenna cable then run it to the wireless radio. (**page 36**)

   b. Connect the antenna cable to the wireless radio.

   c. Connect an Ethernet cable from the wireless radio to the **Radio** connector port on the PoE adapter/switch or the Smart Power Switch.

   d. Connect an Ethernet cable from the **DVR** connector port on the PoE adapter/switch or the Smart Power Switch to the **Ethernet** port on the 4RE DVR.

9. **If you have a VISTA WiFi or V300 kit but NO wireless radio kit**, connect an Ethernet cable from the **DVR** connector port on the Smart Power Switch to the **Ethernet** port on the 4RE DVR.

10. **If you have an MDC kit**, connect an Ethernet cable from one of the following switch connector ports to the MDC/laptop:

    - **PoE switch**: One of the numbered connector ports (for example, **Port 1**)
    - **Smart Power Switch**: **Ethernet** connector port

11. **If you have a modem**, connect an Ethernet cable from one of the following switch connector ports to the modem:

    - **PoE switch**: One of the numbered connector ports (for example, **Port 2**)
    - **Smart Power Switch**: **Base 2** or **Ethernet** connector port (whichever is available)

12. **If you have a HiFi Microphone kit**, install the HiFi Mic and its related components (page 45):
    a. Position and install the HiFi Mic antenna on the windshield.

> ***Note:*** *You may need to install two HiFi Mics in some vehicles. For information on antenna placement in this case, see the HiFi Microphone User Guide.*

    b. Install the HiFi Mic bracket and attach the HiFi Mic base to it.
    c. Connect the HiFi Mic antenna cable to the HiFi Mic base.
    d. Connect the HiFi Mic cable to the HiFi Mic base then run it to the 4RE DVR location (but DO NOT connect the cable).
13. **If you have a VISTA WiFi or V300 kit**, install the VISTA or V300 WiFi Base and its related components (page 44):
    a. Position and install the WiFi Base antenna on the windshield.
    b. Install the WiFi Base bracket and attach the WiFi Base to it.
    c. Connect the WiFi Base antenna cable to the WiFi Base.
    d. Connect the WiFi Base cable to the WiFi Base, run it to the Smart Power Switch, then connect it to the **Base 1** connector port on the switch.
14. Install the **cabin microphone** and run its cable to the 4RE DVR location (but DO NOT connect the cable). (page 46)
15. Install the **GPS antenna** and run its cable to the 4RE DVR location (but DO NOT connect the cable). (page 47)
16. Install the **cabin camera** and any other **secondary cameras**, then run their cables to the 4RE DVR location (but DO NOT connect the cables). (page 26)
17. Position the **external inputs cable** part of the power and external inputs harness (page 48):
    a. Run the DVR connector end of the power and external inputs harness to the 4RE DVR location, but DO NOT connect the harness to the 4RE.
    b. Run the external inputs cable to the best location for the vehicle, according to your installation plan.
    c. **If you installed a PoE adapter (page 31) or a PoE switch (page 33)**, connect the orange and brown wires from the external inputs cable to the appropriate component.
    d. Connect each remaining sense wire in the external inputs cable to the corresponding external device input wire, as needed. (page 49)
18. Install the **system power cable** part of the power and external inputs harness (but DO NOT insert the 7.5 amp fuse in the fuse holder) (page 50):
    a. Run the power cable to the vehicle battery location.
    b. Connect the red and black wire extensions to the red and black (and drain) wires in the power cable.
    c. Connect the red and black ring terminals to the appropriate vehicle battery posts, but DO NOT insert the 7.5 amp fuse in the fuse holder.

19. **If you installed a Smart Power Switch**, install the Smart Power Switch power cable (but DO NOT insert the 7.5 amp fuse in the fuse holder) (page 42).
    a. Position the Smart Power Switch end of the power cable near the Smart Power Switch location, but DO NOT connect it to the switch.
    b. Run the power cable to the vehicle battery location.
    c. Connect the red and black wire extensions to the red and black wires in the power cable, as needed.
    d. Connect the red and black ring terminals to the appropriate vehicle battery posts, but DO NOT insert the 7.5 amp fuse in the fuse holder.
20. Connect the following cables to the **4RE DVR**, as applicable:
    a. Cabin microphone cable to the **Cab Mic** connector port
    b. Display HDMI cable to the **Display** connector port
    c. All camera cables to their appropriate connector ports
    d. HiFi Microphone cable to the **Wireless Mic** connector port
    e. GPS cable to the **GPS** connector port



Note: *If you are mounting the 4RE DVR in the console, you may need to use the HDMI right-angle adapter kit to avoid making sharp bends in the HDMI cables where they connect to the 4RE DVR. For more information and to order the kit, contact WatchGuard Customer Service.*

21. **If you installed a Smart Power Switch**, connect the Smart Power Switch power cable to the **+12 VDC** connector port on the switch.
22. Connect the **system power and external inputs harness** to the **External Inputs/Power** connector port on the 4RE DVR.
23. **If you installed a Smart Power Switch**, insert the 7.5 amp fuse into the Smart Power Switch power cable fuse holder.
24. Insert the **7.5 amp fuse** into the system power cable fuse holder.
25. Test the installation (page 52).

Installing Cameras in the 4RE System

The 4RE Standard system can have up to three cameras in an installation, one front camera and two secondary cameras. The 4RE Elite system can have up to six cameras in an installation, one front camera and five secondary cameras.

WatchGuard offers three types of front camera:

- ZSL (Zero Sightline) (page 25)
- Panoramic X2 HD (page 25)

  The Panoramic X2 HD counts as two cameras in the installation, one front camera and one secondary camera.
- Mini-Zoom (page 26)

Each type is mounted either with a puck (rearview mirror button) adhered to the windshield (below) or to a bracket.

A vehicle installation typically includes one secondary camera facing the back seat (cabin camera), but it can include up to five secondary cameras. (page 26)

Installing the front camera using the puck

If you are using a puck (rearview mirror button) to install the front camera, attach the puck to the windshield using Loctite® 312 adhesive.



Tip: *You can use a hand-held butane torch or lighter to heat the puck. This can help speed up the installation process.*

1. Clean the windshield surface using a microfiber cloth (or something similar), and alcohol or window cleaner.
2. Clean any residue from the puck, using alcohol or window cleaner.



Important! *DO NOT score the surface of the puck. Scoring the puck can keep it from properly adhering to the windshield.*

3. Place the puck in the front camera mount.



Tip: *Do not over-tighten the mount to the puck. Over-tightening causes a slight curve in the puck that keeps it from adhering properly to the windshield.*

4. Determine where exactly on the windshield you want to mount the front camera.

> ***Note:*** *Place the puck as high as possible on the windshield for a better viewing angle.*

5. (Optional) Heat the puck for 10 to 15 seconds, using a lighter or a hand-held butane torch, until it is warm to the touch.

> ***Note:*** *Wipe off any black residue left from the lighter flame.*

The color of the puck changes slightly when it is heated.

6. Carefully spray Loctite® primer on the puck AND the windshield (1 or 2 sprays to cover the area where you are mounting the puck).
7. Let the primer dry.
8. Apply a drop (5/16-inch or pea size) of the Loctite adhesive to the puck.

> ***Tip:*** *Apply enough adhesive that it spreads to every corner of the puck when you press the puck to the glass.*

9. Quickly press the puck with the camera attached to the windshield and hold it there for 60 seconds.
10. Leave the camera in place for at least 10 minutes to allow the adhesive to dry completely.

> ***Note:*** *If the puck does not successfully adhere to the windshield, replace the used puck with a new one and try again.*

11. Connect the HDMI cable to the front camera then run the cable to the 4RE DVR location (but DO NOT connect the cable to the 4RE).
12. When instructed to do so in the full installation workflow on **page 22**, connect the front camera HDMI cable to the **Front** connector port on the 4RE DVR.

> ***Important!*** *Only connect cables when the full installation workflow on* ***page 19*** *instructs you to. Connecting cables out of sequence can damage components.*

Panoramic X2 HD



The Panoramic X2 HD contains two cameras: a rotatable HD (high definition) camera that functions as the front camera in the vehicle, and a fixed panoramic camera that has a very wide field of view and functions as a secondary camera.

You can mount the Panoramic X2 HD camera using one of two options:

- Puck mounted to the windshield just behind the rearview mirror (page 23)
- Bracket mounted to the passenger visor post



Zero Sightline



The Zero Sightline (ZSL) is an HD (high definition) camera that functions as the front camera in the vehicle. It typically mounts in front of the rearview mirror so it does not obstruct the officer's line of sight.

You can mount the ZSL camera using one of two options:

- Puck mounted to the windshield just behind the rearview mirror (page 23)
- Bracket mounted to the passenger visor post



HD Mini Zoom



The HD Mini Zoom camera is an HD (high definition) camera that functions as the front camera in the vehicle. It features a 12X optical zoom.

You can mount the HD Mini Zoom camera using one of two options:

- Puck mounted to the windshield about one inch to the right of the rearview mirror (page 23)
- Bracket mounted to the passenger visor post



Installing the cabin and other secondary cameras

Typically, a vehicle installation includes one secondary camera facing the back seat (cabin camera), but an installation can have up to five secondary cameras.



To install the cabin and other secondary cameras:

1. Mount each secondary camera according to your installation plan.
2. Connect each camera's cable to the camera then run it to the 4RE DVR location but DO NOT connect the cables to the 4RE.
3. When instructed to do so in the full installation workflow on page 22, connect the secondary camera cables to the appropriate connector ports on the 4RE DVR.

Notes for secondary camera installation

Where you connect the secondary cameras to the 4RE DVR depends on which cameras and which version of the 4RE are part of the installation. For two examples of 4RE DVR connections, see *Installing the 4RE DVR* on **page 29**.

Keep the following items in mind when you install secondary cameras:

- If you installed a Panoramic X2 HD camera as your front camera OR you have an **Auxiliary Cameras** connector port (mezzanine card) on the 4RE DVR, you can only connect one camera to port **2** (you cannot use a splitter on camera port **2**)
- If you installed a Panoramic X2 HD camera as your front camera AND you have an **Auxiliary Cameras** connector port (mezzanine card) on the 4RE DVR, you cannot use camera port **2**

If you need more information about connecting secondary cameras to the 4RE, contact WatchGuard customer service.

Installing the 4RE DVR Display

Typically you mount the 4RE Display on a bracket using a RAM® ball mount. The mount has two main parts: a ball that attaches to the display bracket and a ball that attaches to the back of the display. A joint connects the two parts of the mount together.

Tip: *Where you mount the 4RE DVR Display varies from vehicle to vehicle. For more information, see the mounting instructions included with the brackets.*

To install the 4RE DVR Display:

1. Position and install the display bracket.

   Note: *You may have already installed the display bracket when you installed the front camera bracket.*

2. Attach the bracket-side part of the display mount to the display bracket.
3. Remove the back panel from the display and connect the display HDMI cable.
4. Replace the back panel on the display.

   Important! *Make sure that you do not pinch the HDMI cable when you replace the back panel on the display.*



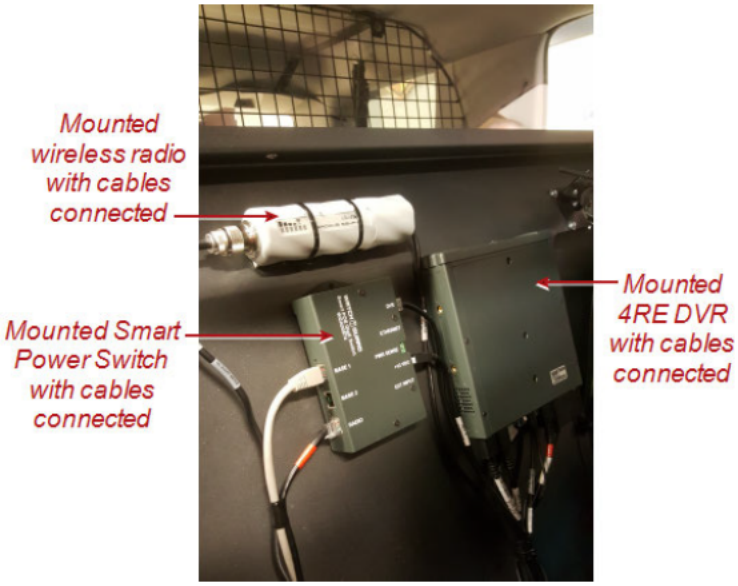
5. Attach the display-side RAM bracket and ball to the back of the display.
6. Attach the display to the display bracket using the mount knuckle joint to connect the two mount parts together.
7. Run the display HDMI cable to the 4RE DVR location, but DO NOT connect it to the DVR.
8. When instructed to do so in the full installation workflow on **page 22**, connect the display HDMI cable to the 4RE DVR.

   Important! *Only connect cables when the full installation workflow on **page 19** instructs you to. Connecting cables out of sequence can damage components.*

Installing the 4RE DVR

How and where you mount the 4RE DVR depends on agency preference as well as the vehicle where you are installing the system. The most common locations for mounting the 4RE DVR include:

- Behind the front seat (photo below)
- In the console
- On an equipment tray in the trunk



To install the 4RE DVR:

1. Install the 4RE DVR bracket.

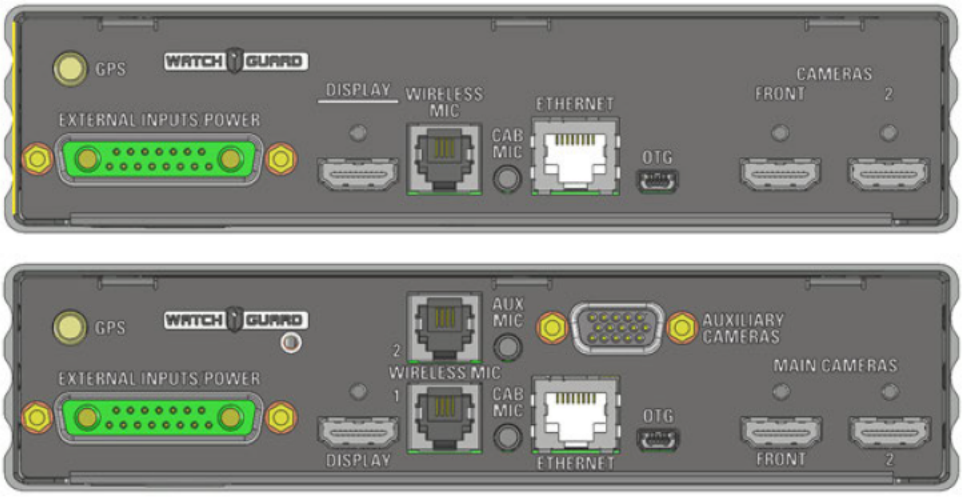
> ***Note:*** *For information about installing the DVR bracket for a particular vehicle, see the mounting instructions included with the bracket.*

2. Position and loosely install the 4RE DVR, but DO NOT connect cables to it.

> ***Important!*** *Only connect cables when the full installation workflow on* **page 19** *instructs you to. Connecting cables out of sequence can damage components.*

3. When instructed to do so in the full installation workflow on page 22, connect cables to the back of the 4RE DVR.

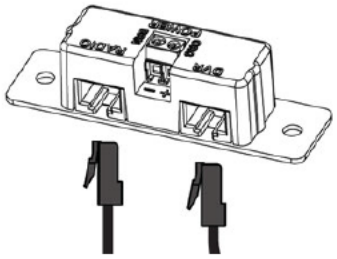
> ***Tip:*** *If you are mounting the 4RE DVR in the console, you may need to use the HDMI right-angle adapter kit to avoid making sharp bends in the HDMI cables where they connect to the 4RE DVR. For more information and to order the kit, contact WatchGuard Customer Service.*



> ***Note:*** *The 4RE DVR you are installing is one of multiple possible versions. Two of the most common variations are pictured above.*

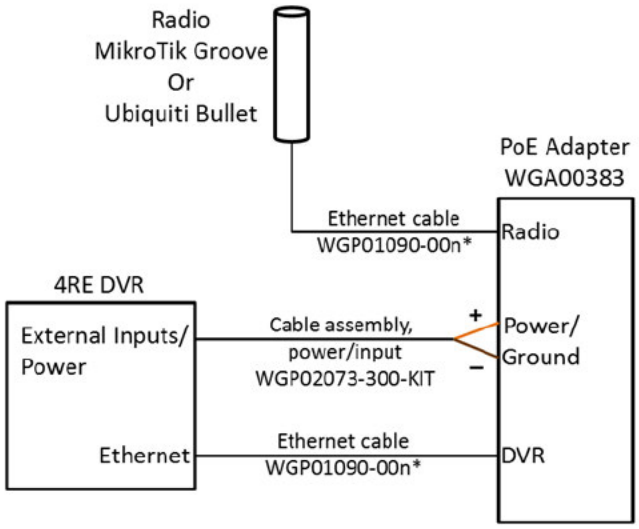
Installing a PoE adapter

Important! *If the system you are installing includes the integrated VISTA or V300 body camera and 4RE DVR components, you must install the Smart Power Switch instead of the PoE adapter. For more information and instructions, see Installing the 4RE/VISTA or 4RE/V300 System on* **page 40***.*



If you are installing a wireless radio in the system, you need to install and connect the PoE (power over Ethernet) adapter. The PoE adapter allows the 4RE DVR to provide power and the data connection for the wireless radio.

Typically you mount the adapter within a few feet of the wireless radio, for example, behind the seat.



* The last digit of the part number changes depending on the length of the Ethernet cable.

Note: *If you need to include an MDC (mobile data computer) or modem in the system, you need to install a PoE switch instead of the adapter. For instructions how to install the PoE switch, see Installing a PoE Switch on* **page 33***.*

To connect the PoE adapter into the system and to the radio:

1. Mount the adapter according to your installation plan, but DO NOT connect any cables.

> ***Important!*** *Only connect cables when the full installation workflow on* *page 19* *instructs you to. Connecting cables out of sequence can damage components.*

2. Locate the two Ethernet cables included in the DVR installation kit.
3. Connect the following cables ONLY when instructed to do so in the full installation workflow on **page 20**:
   a. Connect one Ethernet cable from the **Radio** connector port on the PoE adapter to the wireless radio.

> ***Warning!*** *DO NOT plug in the wireless radio's PoE connector (Ethernet connection) and power up the radio WITHOUT an antenna connected. Powering up the radio without an antenna can damage the radio.*

   b. Connect the other Ethernet cable from the **DVR** connector port on the PoE adapter to the 4RE DVR.

> ***Warning!*** *Make sure you connect the Ethernet cables to the correct ports on the PoE adapter. Plugging the cables in backwards will damage the Ethernet port on the 4RE DVR.*

4. After running the external inputs cable (and when instructed to do so in the full installation workflow on **page 21**), insert the orange (positive 12 volt power) and brown (ground) wires from the external inputs cable into the appropriate labeled holes on the adapter, then tighten down the screws.

> ***Note:*** *For more information on connecting the wires from the external inputs cable, see Connecting the External Inputs Cable on* *page 48**.*

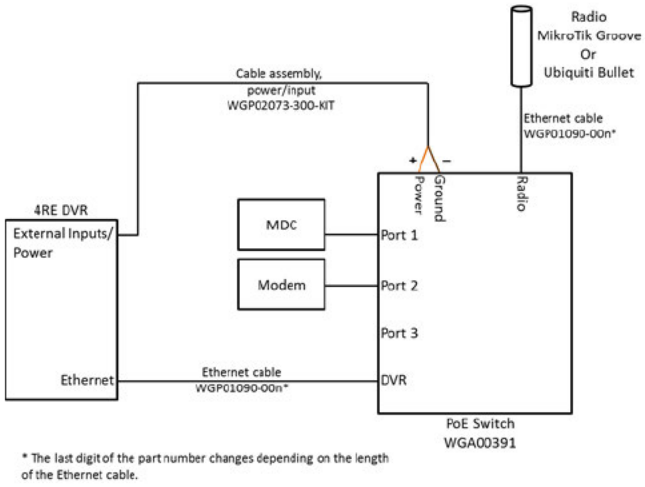
Installing a PoE Switch

Important! *If the system you are installing includes the integrated VISTA WiFi and 4RE DVR components, you must install the Smart Power Switch instead of the PoE switch. For more information and instructions, see Installing the 4RE/VISTA or 4RE/V300 System on* **page 40***.*



If you need to include an MDC (mobile data computer), laptop, or modem (for example, Sierra Wireless®) in the system as well as a wireless radio, you need to install and connect the PoE (power over Ethernet) switch. The PoE switch allows the 4RE DVR to provide power and a data connection for the wireless radio as well as an additional data connection for the MDC/laptop or modem.

Typically you mount the PoE switch within a few feet of the wireless radio, for example, behind the seat.



* The last digit of the part number changes depending on the length of the Ethernet cable.

Note: *If you do not need to include an MDC (mobile data computer) or modem in the system, you only need to install a PoE adapter instead of the switch. For instructions how to install the adapter, see Installing a PoE adapter on* **page 31***.*

To connect the PoE switch into the system:

1. Mount the switch according to your installation plan, but DO NOT connect any cables.

> ***Important!*** *Only connect cables when the full installation workflow on* *page 19* *instructs you to. Connecting cables out of sequence can damage components.*

2. Locate the two Ethernet cables included in the DVR installation kit and the additional Ethernet cables included with the MDC package and/or modem.
3. Connect the following cables ONLY when instructed to do so in the full installation workflow on **page 19**:
   a. Connect one Ethernet cable from the **Wireless Radio** connector port on the PoE switch to the wireless radio.

> ***Warning!*** *DO NOT connect the wireless radio's Ethernet connection or power up the radio WITHOUT an antenna connected. Powering up the radio without an antenna can damage the radio.*

   b. Connect one Ethernet cable from the **DVR** connector port on the PoE switch to the 4RE DVR.

> ***Warning!*** *Make sure you connect the Ethernet cables to the correct ports on the PoE switch. Plugging the cables into the wrong ports will damage the Ethernet port on the 4RE DVR.*

   c. As needed, connect one Ethernet cable from any of the numbered ports on the PoE switch to the MDC/laptop (or laptop docking station).

> ***Warning!*** *Make sure you only connect the MDC/laptop to one of the numbered ports on the PoE switch. Plugging the MDC cable into the wrong port on the switch will damage the MDC/laptop.*

   d. As needed, connect one Ethernet cable from any of the numbered ports on the PoE switch to the modem.
4. After running the external inputs cable (and when instructed to do so in the full installation workflow on **page 21**), insert the orange (positive 12 volt power) and brown (ground) wires from the external inputs cable into the appropriate labeled holes on the switch, then tighten down the screws.

> ***Note:*** *For more information on connecting the wires from the external inputs cable, see Connecting the External Inputs Cable on* *page 48**.*

Installing the Wireless Radio

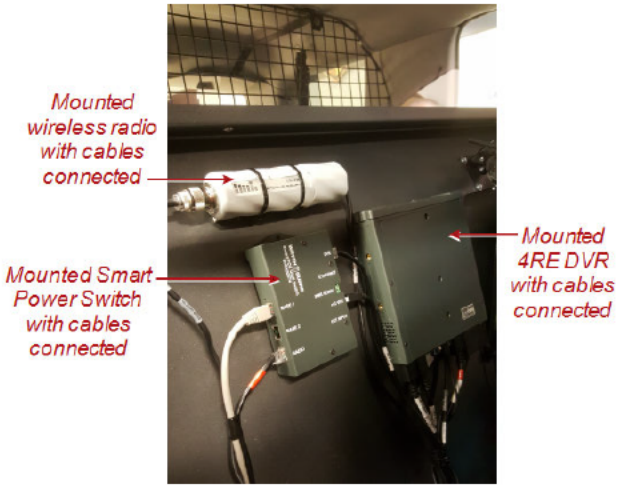
Important! *WatchGuard recommends that wireless radios be configured before you mount them in the vehicle. Typically, radios purchased from WatchGuard are configured before they leave the factory. If you have chosen to configure your own wireless radios, before starting the configuration process, contact WatchGuard Customer Service for instructions.*

WatchGuard provides the following type of wireless radio:

- MikroTik Groove (page 39)

Note: *If you are reinstalling older equipment, you may have a Ubiquiti® Bullet™ radio. If you need information or instructions specific to the Bullet radio, contact WatchGuard Customer Service.*

Typically you mount the wireless radio near the switch and/or 4RE DVR, for example, behind the front seat, using zip ties.



Note: *No mounting hardware is included with the wireless radio.*

To install the wireless radio:

1. Mount the wireless radio according to your installation plan, but DO NOT connect any cables.

> ***Important!*** *Make sure you mount the wireless radio in a position where you can easily see its LEDs. The LEDs are needed for diagnostic purposes.*

2. Mount the wireless radio antenna. (below)
3. Run the antenna cable to the wireless radio then connect it.

> ***Warning!*** *DO NOT plug in the wireless radio's PoE connector (Ethernet connection) and power up the radio WITHOUT an antenna connected. Powering up the radio without an antenna can damage the radio.*

4. When instructed to do so in the full installation workflow on **page 20**, connect an Ethernet cable from the radio connector port on the switch or the PoE adapter to the wireless radio.

> ***Warning!*** *Make sure you connect the Ethernet cable to the correct port on the switch or adapter. Plugging the cables into the wrong ports will damage the Ethernet port on the 4RE DVR.*

Mounting the wireless radio antenna

Typically, you mount the radio antenna on the roof or trunk of the vehicle.

> ***Important!*** *WatchGuard recommends that you keep 9 inches between the wireless radio antenna and other antennas. You must keep a minimum of 6 inches between antennas.*

You route the antenna cable into the vehicle to the location where you plan to mount the wireless radio. You can choose from two different types of radio antenna mounts:

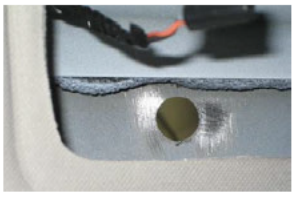
- Through-hole antenna (NMO mount) which requires that you drill a 3/4-inch hole through the vehicle roof

  The example installation in this section shows an NMO mount antenna.
- Magnetic mount which does not require that you drill a hole

> ***Important!*** *WatchGuard Video recommends that you use the NMO mount antenna because it provides better signal strength.*

To install an NMO mount radio antenna:

1. Access the roof of the vehicle in your preplanned location (for example, through the rear seat dome light or by removing the headliner).
2. Drill a 3/4-inch hole for the antenna cable.
3. Sand the paint off the metal around the interior hole to ensure a good ground.



4. Remove the NMO nut from the radio antenna cable.
5. Starting with the radio-connector end, feed the antenna cable through the exterior hole in the vehicle until only the antenna mount (NMO-connector) end of the cable remains outside the vehicle.



6. Tilt the antenna mount end to guide it through the exterior hole, then center the flange in the hole.



7. Make sure that the antenna mount ridges are in contact with the bare metal (from your sanding) inside the vehicle.



8. On the antenna mount outside the vehicle, reattach the NMO nut, with the O-ring facing down to create a seal.



9. Tighten the nut with a 24mm or 15/16-inch open-end wrench, making sure that the mount stays centered in the hole and does not turn and kink the cable.

Tip: *To keep the cable from turning and kinking, use needle-nose pliers in the holes on the antenna mount to anchor the mount while you tighten the NMO nut.*



Warning! *DO NOT tighten the NMO nut using channel-lock pliers. Tightening the NMO nut using a channel-lock pliers can damage the nut and cause an unreliable wireless signal.*

10. Inside the vehicle, route the radio-connector end of the antenna cable to the location where you plan to mount the radio, making sure that you leave enough slack to avoid kinks.
11. Attach the antenna connector to the radio.



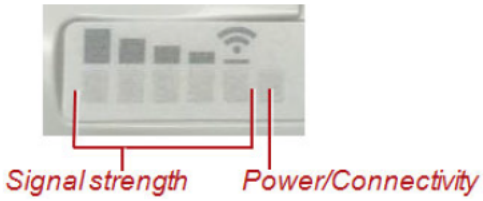
Warning! *DO NOT plug in the wireless radio's PoE connector (Ethernet connection) and power up the radio WITHOUT an antenna connected. Powering up the radio without an antenna can damage the radio.*

MikroTik Groove

Warning! *Do not connect the wireless radio's Ethernet connection or power up the radio without an antenna connected. Powering up the radio without an antenna can damage the radio.*



To verify that the MikroTik Groove wireless radio is working properly, check the LEDs on the side of the device:



- **Power/Connectivity LED**: When lit, shows that the radio has power and is connected to the 4RE DVR system

Tip: *To see whether the Groove radio is communicating successfully with the 4RE DVR, after the 4RE is configured, navigate to the* ***Wireless*** *screen on the 4RE (press* ***Menu*** *on the Control Panel, then touch* ***Settings*** *>* ***Diagnose*** *>* ***Wireless*** *on the Screen) and look for the* ***Access Connected*** *value. If the value is* ***Yes****, the Groove radio can see the 4RE to communicate with it.*

- **Signal strength LEDs**: When lit, shows that the radio is associated with the agency's access point

  All of the LEDs on the Groove radio are green when lit. The signal between the radio and the access point is strongest when all five signal-strength LEDs are lit.

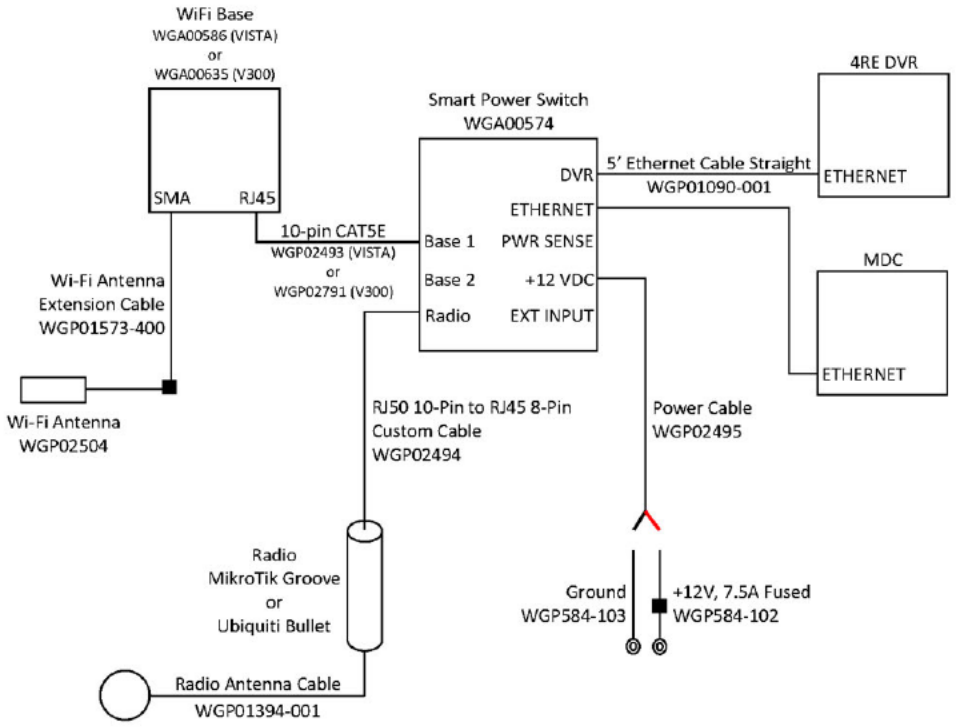
Installing the 4RE/VISTA or 4RE/V300 System

If your vehicle installation includes the VISTA or V300 body camera with the 4RE, you need to install:

- Smart Power Switch (page 41)
- VISTA or V300 WiFi Base (page 44)

The Smart Power Switch is typically mounted near the 4RE DVR. The WiFi Base is typically mounted on or near the passenger visor post.

Important! *Only connect cables when the full installation workflow on page 19 instructs you to. Connecting cables out of sequence can damage components.*

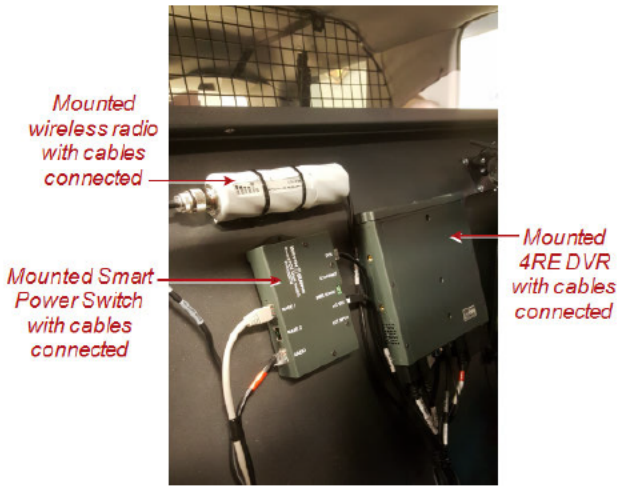


Installing the Smart Power Switch

If the system you are installing includes the VISTA or V300 body camera and 4RE DVR components, you must install the Smart Power Switch instead of the PoE (power over Ethernet) switch (page 33) or adapter (page 31).

The Smart Power Switch is required for the integrated body camera and 4RE to form a recording group. As part of the local recording group network, the Smart Power Switch:

- Functions as the central connection point
- Intelligently manages power
- Functions as the local network DHCP server



Typically you mount the Smart Power Switch within a few feet of the wireless radio, for example, in the console or behind the seat.

Note: *For a cabling diagram showing the 4RE/VISTA or 4RE/V300 system, see Installing the 4RE/VISTA or 4RE/V300 System on* *page 40**.*

To connect the Smart Power Switch into the system:

1. Mount the switch according to your installation plan, but DO NOT connect any cables.

   Important! *Only connect cables when the full installation workflow on* *page 19* *instructs you to. Connecting cables out of sequence can damage components.*

2. Locate the two Ethernet cables included in the DVR installation kit and the additional Ethernet cables (as needed) for the MDC package or modem (for example, Sierra Wireless®).
3. Connect the following cables only when instructed to do so in the full installation workflow on page 20:
   a. Connect one Ethernet cable from the **Radio** connector port on the Smart Power Switch to the wireless radio.

      Warning! *Do not connect the wireless radio's Ethernet connection or power up the radio without an antenna connected. Powering up the radio without an antenna can damage the radio.*

b. Connect one Ethernet cable from the **DVR** connector port on the Smart Power Switch to the 4RE DVR.

> ***Warning!*** *Make sure you connect the Ethernet cables to the correct ports on the Smart Power Switch. Plugging the cables into the wrong ports will damage the Ethernet port on the 4RE DVR.*

c. As needed, connect one Ethernet cable from the **Ethernet** connector port on the Smart Power Switch to the MDC/laptop.

> ***Note:*** *If you are installing a laptop docking station, connect the cable from the switch to the Ethernet port on the docking station. For more information, see the manufacturer's documentation for the docking station.*

> ***Warning!*** *Make sure you only connect the MDC/laptop to the* ***Ethernet*** *connector port on the Smart Power Switch. Plugging the MDC cable into the wrong port on the switch will damage the MDC/laptop.*

d. As needed, connect one Ethernet cable from either the **Ethernet** or the **Base 2** connector port (whichever is available) on the Smart Power Switch to the modem.

4. After running the WiFi Base cable (and when instructed to do so in the full installation workflow on page 21), connect the base cable to the **Base 1** connector port on the Smart Power Switch.
5. When instructed to do so in the full installation workflow on page 22, install the Smart Power Switch power cable (below).

Installing the Smart Power Switch power cable

> ***Warning!*** *Only connect cables when the full installation workflow on* *page 19* *instructs you to. Connecting cables out of sequence can damage components.*

When you install the Smart Power Switch power cable, connect it directly to the vehicle battery. To install the Smart Power Switch power cable:

1. Route the power cable to the vehicle battery.

> ***Important!*** *Use the firewall holes and grommets provided by the vehicle manufacturer to route the cable to the battery. Consult your vehicle manufacturer's documentation for specific information.*

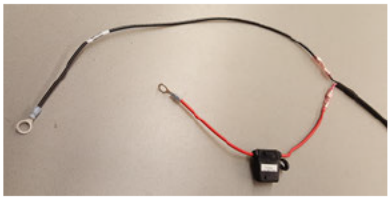
2. Pull the power cable, including any excess cable, toward the battery, leaving some slack for a drip loop.

3. Wind up and tie off or cut the excess power cable.
4. Strip back the sheath on the power cable and its red (positive) and black (ground) wires.



5. Crimp the black (ground) wire to the provided black (ground) wire extension with the attached ring terminal.

> ***Tip:*** *Use butt splices when you connect the wires to ensure good connection.*



6. Crimp the red (positive) wire to the provided red (positive) 7.5 amp fuse holder with the attached ring terminal but DO NOT insert the 7.5 amp fuse in the fuse holder.
7. Connect the red (positive) and black (ground) ring terminals to their vehicle battery posts.
8. When instructed to do so in the full installation workflow on page 22, connect the Smart Power Switch power cable to the **+12 VDC** connector port on the Smart Power Switch.
9. When instructed to do so in the full installation workflow on page 22, insert the 7.5 amp fuse in the fuse holder.

> ***Warning!*** *DO NOT insert the 7.5 amp fuse until you have finished installing and connecting all the system equipment. Inserting the fuse before you finish the full installation can damage the system.*

Installing the VISTA or V300 WiFi Base

If the system you are installing includes the VISTA WiFi or V300 kit, you must install the VISTA or V300 WiFi Base.



The WiFi Base is required for the integrated body camera and 4RE DVR to form a recording group. As part of the local recording group network, the WiFi Base:

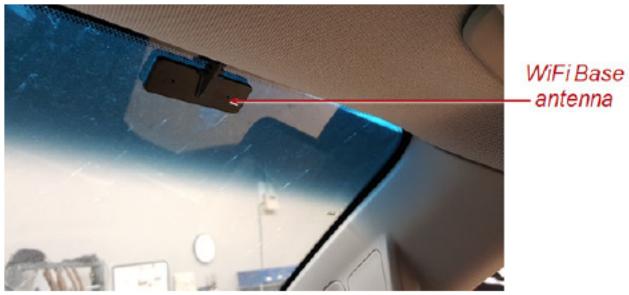
- Pairs with the VISTA WiFi or V300 body camera so the camera can associate with the local recording group
- Acts as a Wi-Fi access point (hotspot) for the VISTA WiFi or V300 camera

Typically, you mount the WiFi Base on or near the passenger visor post, but the universal bracket can be mounted in almost any location in the vehicle. If you are also installing the HiFi Microphone (HiFi Mic), you can install both bases next to each other on a bracket designed for two bases.

Note: *For a cabling diagram showing the 4RE/VISTA or 4RE/V300 system, see Installing the 4RE/VISTA or 4RE/V300 System on* **page 40***.*

To install the VISTA or V300 WiFi Base:

1. Position and install the WiFi Base antenna on the windshield inside the vehicle at least 2 to 3 inches away from any metal.



Tip: *For best performance, install the WiFi base antenna in the upper center area of the windshield, behind the rearview mirror.*

2. Install the WiFi Base bracket (if not already installed) and attach the WiFi Base to it.
3. Run the WiFi Base antenna cable to the WiFi Base and connect it.
4. Connect the WiFi Base cable to the WiFi Base then run it to the Smart Power Switch location.
5. When instructed to do so in the full installation workflow on **page 21**, connect the WiFi Base cable to the **Base 1** connector port on the Smart Power Switch.

Installing Microphones in the System

WatchGuard provides two types of microphones for the 4RE system:

- Wireless (HiFi Microphone) (below)
- Cabin (page 46)

The officer wears the HiFi Microphone (HiFi Mic) during his shift then docks it in the HiFi Mic base in the vehicle to charge. The HiFi Mic base mounts on a bracket installed in a location that the officer can easily reach.

The cabin microphone mounts in a location where it can pick up any audio inside the vehicle.

Installing the HiFi Microphone



Typically, you mount the HiFi Microphone (HiFi Mic) base on or near the passenger visor post, but the universal bracket can be mounted in almost any location in the vehicle, as needed.

To install the HiFi Mic:

1. Position and install the HiFi Mic antenna horizontally in the upper right corner of the windshield inside the vehicle.



Warning! *Do not mount the HiFi Mic antenna vertically. If you mount the antenna vertically, the HiFi Mic will have very poor signal strength.*

Note: *If you need to install two HiFi Mics in a vehicle, for information on antenna placement, see the HiFi Microphone User Guide.*

2. Install the HiFi Mic bracket and attach the HiFi Mic base to it.
3. Run the HiFi Mic antenna cable to the HiFi Mic base and connect it.
4. Connect the HiFi Mic cable to the HiFi Mic base then run it to the 4RE DVR location (but DO NOT connect the cable).
5. When instructed to do so in the full installation workflow on page 22, connect the HiFi Mic cable to the **Wireless Mic** connector port on the 4RE DVR.

Installing the cabin microphone

You should mount the cabin microphone in a location where it can pick up any audio inside the vehicle.



Important! *Do not mount the cabin microphone within 5 to 6 inches of the wireless microphone. Mounting the cabin microphone too close to the HiFi Mic can cause interference in the recorded audio.*

To install the cabin microphone:

1. Mount the cabin microphone according to your installation plan.
2. Run the cabin microphone cable to the 4RE DVR location (but DO NOT connect the cable).
3. When instructed to do so in the full installation workflow on page 22, connect the cabin microphone cable to the **Cab Mic** connector port on the 4RE DVR.

Warning! *Make sure you connect the cabin microphone cable to the 4RE DVR before you power the DVR ON. Connecting the cabin microphone cable after you power ON the DVR can damage the cabin microphone connector port and the 4RE DVR.*

Installing the GPS Antenna

You should mount the GPS antenna with line-of-sight to the sky, for example, exterior roof, exterior trunk, or interior dashboard.

Tip: *WatchGuard recommends that you mount the GPS antenna in the center of the dashboard no more than 3 inches from the windshield and not blocked by any window tint.*

To install the GPS antenna:

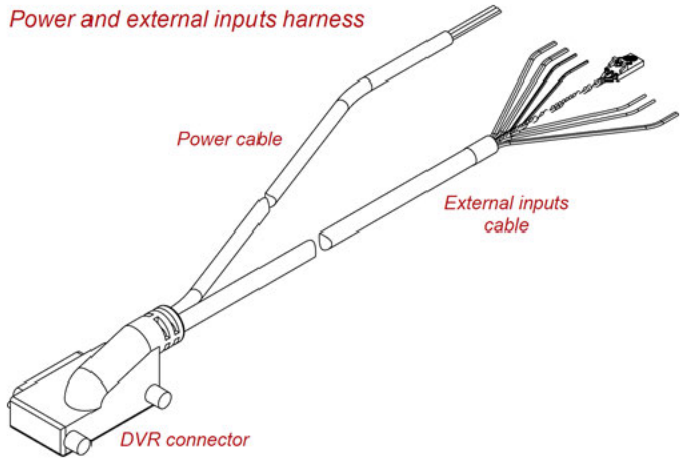
1. Mount the GPS antenna according to your installation plan.
2. Run the GPS antenna cable to the 4RE DVR location (but DO NOT connect the cable).
3. When instructed to do so in the full installation workflow on page 22, connect the GPS antenna cable onto the **GPS** connector port on the 4RE DVR.

Tip: *Due to different vehicle and windshield manufacturers, in some cases when the GPS antenna is mounted on the dashboard, the antenna does not consistently lock in on satellites. This can cause the 4RE to record incorrect speeds and possibly trigger an erroneous recorded event with the over-speed trigger.*

In this case, remount the GPS antenna outside the vehicle on the roof or the trunk in line-of-sight to the sky.

Connecting the External Inputs Cable

Warning! *Only connect cables when the full installation workflow on* **page 19** *instructs you to. Connecting cables out of sequence can damage components.*



The power and external inputs harness connects the 4RE DVR to the vehicle battery and to external device inputs, for example, ignition, emergency lights, and siren.

The external inputs cable part of the harness connects the 4RE DVR sense wires with the vehicle external device inputs.

Note: *For instructions how to connect the power cable to the vehicle battery, see Connecting the System Power Cable to the Vehicle Battery on* **page 50***.*

The sense wires in the external inputs cable monitor the external device inputs for voltage (8-12 volts) and no voltage (0 volts). When an external input wire senses voltage from an external device, the 4RE starts a recorded event, if configured to do so in the agency's Evidence Library software. (0 volts signals to the 4RE that it should prompt the user to stop the event, if configured to do so.)

The presence of voltage on the sense wire also signals to the system to add the external device activation information to the metadata file.

Connect each sense wire in the external inputs cable to the corresponding external device input wire:



Tip: *Where possible, use butt splices when you connect the wires to ensure good connection and consistent voltage.*

- **Ignition (white)**: The white wire senses whether the ignition is on or off

  Connect the white wire to a feed (switched ignition accessory wire) that provides positive 12 volts when the vehicle ignition is ON and 0 volts when the vehicle ignition is OFF. A fuse link with a 1-amp fuse is provided to connect the ignition feed with the ignition sense wire from the external inputs cable.

- **Emergency lights (blue with white stripe)**: The blue wire with the white stripe senses whether the emergency lights have been activated

  Connect the blue wire with the white stripe to a positive 12-volt switched power source that provides voltage when the overhead lights are activated.

  Note: *Some manufacturers of older-type light bars use negative 12 volt or ground triggers. In those cases, you may need to incorporate an additional relay into the wiring scheme to provide positive 12 volt power to the external input wire.*

- **Siren (pink and green)**: The pink and green wires sense whether the siren has been activated

  Connect the green wire to the siren speaker ground feed and the pink wire to the positive siren speaker feed. When the siren is activated, the siren input (pink and green wires together) senses the voltage.

- **Auxiliary (solid blue)**: The solid blue wire senses whether an auxiliary device has been activated

  If an auxiliary device is to be used, connect the solid blue wire to a source that provides positive 12-volt switched power when the auxiliary device is activated, for example, when the electric release button is pressed on a shotgun mount or an electric K-9 kennel door is released.

- **Brake input (black with white stripe)**: The black wire with the white stripe senses whether the brakes are being applied

  Connect the black wire with the white stripe to a positive 12-volt switched power source that is activated when the brake pedal is applied. (When the brakes are applied, the wire should get 12 volts.)

- **Power and ground (orange and brown)**: The orange and brown wires provide power and ground (respectively) for the wireless radio using the PoE (power over Ethernet) adapter or PoE switch

  Connect the orange wire (positive 12 volt power) and the brown wire (ground) to the appropriate labeled connection points on either the PoE adapter (page 31) or the PoE switch (page 33).

  If you are installing the equipment associated with the integrated VISTA or V300 body camera and 4RE DVR system, the Smart Power Switch takes the place of the PoE adapter or PoE

switch. You connect the Smart Power Switch to another power source (vehicle battery), NOT the orange and brown wires from the external inputs cable (page 42).

- **Radar interface (purple/black/gray) connector**: The purple-, black-, and gray-wired connector provides a two-way interface between the 4RE DVR and the radar unit

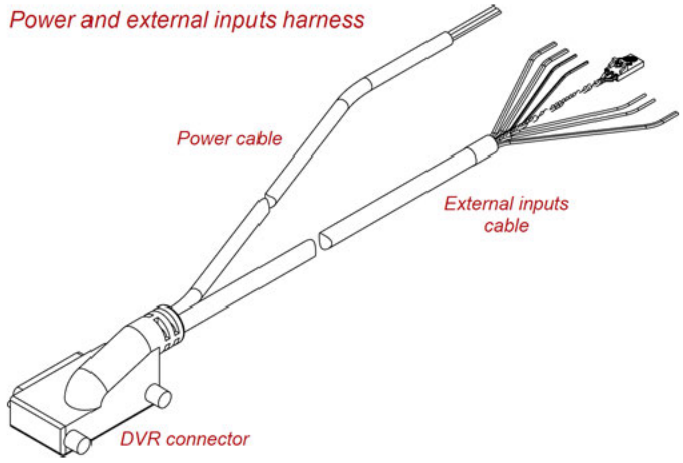
  Connect the purple-, black-, and gray-wired connector with the radar interface cable coming from the radar unit. For more information, see the installation instructions included with the radar interface cable.

Tip: *Each of the sense wires in the external inputs cable is labeled with the name of the external device input it should connect to. If you need to cut the cable (for example, because it is too long for the space you have), bind the cut labeled ends together and save them to serve as the key for the connections.*

For more information about connecting the external inputs cable to the various external device input wires, see the WatchGuard installation poster.

Connecting the System Power Cable to the Vehicle Battery

Warning! *Only connect cables when the full installation workflow on page 19 instructs you to. Connecting cables out of sequence can damage components.*



The system power and external inputs harness connects the 4RE DVR to the vehicle battery and to external device inputs, for example, ignition, emergency lights, and siren.

The system power cable part of the harness connects the 4RE to the vehicle battery.

Note: *For instructions how to connect the external inputs cable to the input device sense wires, see Connecting the External Inputs Cable on page 48.*

To connect the system power cable to the vehicle battery:

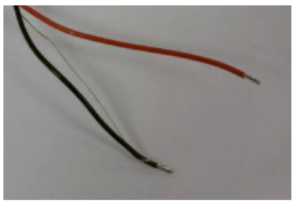
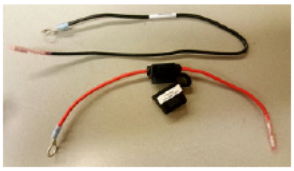
1. Route the cable from the passenger compartment through the firewall into the engine bay.

> ***Important!*** *Use the firewall holes and grommets provided by the vehicle manufacturer to route the cable into the engine bay. Consult your vehicle manufacturer's documentation for specific information.*

> ***Note:*** *If the vehicle battery is not in the engine bay, route the power cable to the battery's location (for example, the trunk) using the holes and grommets provided by the manufacturer throughout the vehicle.*

2. In the engine bay, pull the power cable, including any excess cable, toward the battery, leaving some slack for a drip loop.
3. Wind up and tie off or cut the excess power cable.
4. Strip back the sheath on the power cable and its red (positive) and black (ground) wires.
5. Twist the black (ground) and non-insulated silver drain wires together, then crimp them to the provided black (ground) wire extension with the attached ring terminal.

> ***Tip:*** *Where possible, use butt splices when you connect the wires to ensure good connection.*

6. Crimp the red (positive) wire to the provided red (positive) 7.5 amp fuse holder with the attached ring terminal.
7. Connect the red (positive) and black (ground) ring terminals to their vehicle battery posts.
8. When instructed to do so in the full installation workflow on page 22, connect the system power and external inputs harness to the **External Inputs/Power** connector port on the 4RE DVR.
9. When instructed to do so in the full installation workflow on page 22, insert the 7. 5 amp fuse in the fuse holder.

> ***Warning!*** *DO NOT insert the 7.5 amp fuse until you have finished installing and connecting all the system equipment. Inserting the fuse before you have finished the full installation can damage the system.*

Testing the System Installation

Important! *Make sure that you have finished all the steps in the recommended installation workflow on page 19 before you test the installation.*

To test that all components are properly installed and connected:

1. Power on the system.

   Note: *The system may power on when you insert the 7.5 amp fuse.*

2. Verify that the 4RE Display Screen shows streams from all of the installed cameras.
3. Test the touch screen.
   a. Press **Menu** on the 4RE Display Control Panel.
   b. Touch any button on the Display Screen.
   c. Verify that the correct screen opens.
4. Test the HiFi Microphone (HiFi Mic) audio, as applicable:
   a. Power on the HiFi Mic.
   b. Dock the HiFi Mic so it synchronizes with the base.
   c. Undock the mic, and press the talk button.
   d. Verify that the wireless microphone icon appears on the Display Screen.
   e. Press the Volume control, touch **Advanced** on the Display Screen, then turn up the wireless microphone volume to verify the audio.

      Tip: *Turn the wireless microphone volume back to **0** after you have finished verifying the audio.*

   f. Press **Stop** to end the recorded event.
5. Verify that the external inputs are correctly connected:
   a. Press **Menu** on the Display Control Panel, then touch **Status** > **Device** on the Display Screen.
   b. Activate each input you connected, for example, **Siren**.
   c. Verify that each input shows **On** when you activate it.

6. Verify the body camera system connection:
   a. Dock VISTA or V300 in its WiFi Base so it pairs with the base.
   b. Press **Menu** on the Display Control Panel, then touch **Status** > **VISTA** on the Display Screen.
   c. Verify that the camera appears in the **VISTA** list.

   > ***Note:*** *Both V300 and VISTA appear in the* ***VISTA*** *list.*

7. Verify the wireless radio connection, as applicable:
   a. Check the LEDs on the wireless radio for power and connectivity.

      For information on the MikroTik Groove radio, see *MikroTik Groove* on page 39.
   b. Check the wireless signal icon on the Display Screen.
   c. Press **Menu** on the Display Control Panel, then touch **Settings** > **Diagnose** > **Wireless** on the Display Screen.
   d. Verify that the **Access Connected** value is **Yes**.
8. Create one or more test recorded events:
   a. Press **Record** on the Display Control Panel.
   b. Allow the event to continue for at least 15 seconds.
   c. Press **Stop** on the Display Control Panel to stop the event.
9. Test recorded event playback with audio:
   a. Press **Review** on the Display Control Panel.
   b. Select an event on the Display Screen, then touch **Details** > **Play**.
   c. Press **Volume +** on the Display Control Panel to hear the audio play back with the video.
10. If you have an Evidence Library configuration, load it on the 4RE DVR and verify the configuration items.

    For more information, see the agency's Evidence Library documentation.

This page intentionally left blank.

Appendix A: Cellular LTE Upload

WatchGuard supports uploading recorded events to Evidence Library 4 Web (EL4 Web) or Evidence Library (EL), from the vehicle, over a cellular connection using the following cellular routers:

- Sierra Wireless® AirLink® MG90 High Performance Multi-Network Vehicle Router
- Cradlepoint COR IBR900 LTE router



Note: *See the manufacturer's instructions for installing the routers in the vehicle.*

WatchGuard also supports upload over a cellular connection that does not require a stand-alone LTE router. Supported configurations include:

- LTE-capable MDC (mobile data computer) or laptop
- MDC/laptop with a USB dongle LTE modem attached
- MDC/laptop with an LTE MiFi device attached

For information about setting up a system for cellular upload, contact WatchGuard Customer Service.

Appendix B: WatchGuard Mobile LPR

WatchGuard Mobile LPR (license plate recognition) uses vehicle license plate detection to provide real-time information to in-vehicle officers. The LPR system uses a WatchGuard-branded version of Vigilant's CarDetector software on the MDC (mobile data computer) in combination with WatchGuard and/or Vigilant cameras and an additional processor, depending on the version installed.

Note: *For information about adding WatchGuard Mobile LPR to a 4RE in-car video system, contact WatchGuard Customer Service.*

The system compares license plate scans to hotlists maintained by the agency, shared by other nationwide agencies, and subscribed to (for example, from the FBI National Crime Information Center (NCIC)). The officer receives visual and audible alerts when a hotlist match is made.

Depending on the installed version, the system scans license plates only when the vehicle is stopped (for example, during traffic stops) or also while the vehicle is moving (for example, while patroling).

WatchGuard Mobile LPR is available in three versions:

- **Officer Safety Basic**

  The **Basic** version uses only the 4RE front camera (Panoramic X2, Zero Sightline, or Mini Zoom Camera) to scan one license plate at a time. The software scans the front camera HD video stream while vehicles are stopped to determine whether a license plate is of interest.

  Internet access is required to upload data and download updates. The GPS antenna included with the 4RE system provides the location data saved with plate detections.

- **Officer Safety Advanced**

  The **Advanced** version adds two Vigilant LPR/ANPR (automatic number plate recognition) dual-lens LPR cameras and supporting equipment (PoE switch, cables) to enable active scanning of multiple license plates while vehicles are moving.

- **Officer Safety Advanced +**

  The **Advanced +** version adds capability for up to two more Vigilant LPR/ANPR cameras and a VLP (Vigilant Linux processor) unit (plus supporting equipment). (The processor is required to support the increased load from any added cameras and the state, make, and model image scanning that also comes with this version.)

  The VLP unit includes an additional GPS antenna that provides the location data saved with plate detections.

Note: *See the WatchGuard Mobile LPR product documentation for instructions to install and use each of the versions.*

Index

4
4RE DVR
in workflow
connecting cables, 22
mounting DVR, 19
installing, 29
4RE DVR Display
in workflow, 19
installing, 28
A
ALPR, 56
ANPR, 56
antennas
GPS
in workflow, 21
installing, 47
V300
in workflow, 21
installing, 44
VISTA WiFi
in workflow, 21
installing, 44
wireless microphone
in workflow, 21
mounting, 15, 45
wireless radio
in workflow, 20
mounting, 37
audience, 5
auxiliary input
connecting, 49
in workflow, 21
B
base
microphone
in workflow, 21
installing, 45
V300
in workflow, 21
installing, 44
VISTA WiFi
in workflow, 21
installing, 44
best practices, 14
brackets, 9
brakes input
connecting, 49
in workflow, 21
button installation, 23
C
cabin camera
in workflow, 21
installing, 26
cabin microphone
in workflow, 21
installing, 46
cables
connections, 15
external inputs, 48
HDMI, 14
power, 15
in workflow, 21-22
installing, 42, 50
V300, 40
VISTA WiFi, 40
VISTA XLT, 40
cameras
cabin
in workflow, 21
installing, 26
front
HD Mini Zoom, 26
in workflow, 19
installing, 23
Panoramic X2 HD, 25
Zero Sightline, 25
secondary
in workflow, 21
installing, 26
notes, 27
CarDetector, 56
cellular upload, 55
certification, 6
computer
cellular upload, 55
in workflow, 20
configuring wireless radios, 35

cradle
microphone
in workflow, 21
installing, 45
V300
in workflow, 21
installing, 44
VISTA WiFi
in workflow, 21
installing, 44
D
display
in workflow, 19
installing, 28
dock
microphone
in workflow, 21
installing, 45
V300
in workflow, 21
installing, 44
VISTA WiFi
in workflow, 21
installing, 44
DVR
in workflow
connecting cables, 22
mounting DVR, 19
installing, 29
DVR display
in workflow, 19
installing, 28
E
emergency lights
connecting, 49
in workflow, 21
equipment list, 10
external inputs
connecting, 48
in workflow, 21
F
front camera
HD Mini Zoom, 26
in workflow, 19
installing, 23
Panoramic X2 HD, 25
Zero Sightline, 25
full workflow, 19
fuses
in workflow, 22
installing, 43, 51
G
GPS antenna
in workflow, 21
installing, 47
Groove, 39
in workflow, 20
installing, 36
LEDs, 39
Groove antenna
in workflow, 20
mounting, 36
H
HD cameras
HD Mini Zoom, 26
in workflow, 19
installing, 23
Panoramic X2 HD, 25
Zero Sightline, 25
HD Mini Zoom camera, 26
HDMI cables, 14
handling, 14
right-angle adapters, 14, 30
heating puck, 23
HiFi Microphone
in workflow, 21
installing, 45
I
ignition
connecting, 49
in workflow, 21
inputs
auxiliary, 49
brakes, 49
cable, 48
connecting, 48
emergency lights, 49
ignition, 49
in workflow, 21
power and ground, 49
radar interface, 50
siren, 49
installation poster, 9
instructions, full install, 19

integrated V300, 40
integrated VISTA, 40
intended audience, 5
L
laptop
  cellular upload, 55
  in workflow, 20
LEDs, Groove, 39
license plate recognition, 56
lights
  connecting, 49
  in workflow, 21
LPR, 56
LTE
  MiFi device, 55
  upload, 55
M
MDC
  cellular upload, 55
  in workflow, 20
  Mobile LPR, 56
microphone antenna
  in workflow, 21
  mounting, 15
microphones
  cabin
    in workflow, 21
    installing, 46
  wireless
    in workflow, 21
    installing, 45
MiFi device, LTE, 55
MikroTik, 39
  in workflow, 20
  installing, 36
MikroTik antenna
  in workflow, 20
  installing, 36
mirror button installation, 23
mobile data computer
  cellular upload, 55
  in workflow, 20
modem
  cellular, 55
  in workflow, 20
N
NMO mount antenna, 37
O
Officer Safety
  Advanced, 56
  Advanced +, 56
  Basic, 56
order of installation, 19
overview poster, 9
P
Panoramic X2 HD camera, 25
parts list, 10
planning installation, 9
PoE adapter
  in workflow, 20
  installing, 31
PoE switch
  in workflow, 20
  installing, 33
poster, 9
power and ground, inputs cable, 49
power cables, 15
  Smart Power Switch
    in workflow, 22
    installing, 42
  system
    in workflow, 21
    installing, 50
power over Ethernet adapter
  in workflow, 20
  installing, 31
power over Ethernet switch
  in workflow, 20
  installing, 33
pre-installation checklist, 9
prerequisites, 9
puck installation, 23
R
radar interface
  connecting, 50
  in workflow, 21
radio
  configuring, 35
  Groove, 39
  in workflow, 20
  installing, 36
  types, 35
radio antenna
  in workflow, 20

mounting, 36
Reaper cameras, 56
rearview mirror button installation, 23
requirements, 14
resources, 6
right-angle adapters, HDMI cables, 14, 30
roof antenna, 37
router, 55

S

schematic
installation poster, 9
V300 system, 40
VISTA WiFi system, 40
VISTA XLT system, 40
scoring the puck, 23
secondary cameras
in workflow, 21
installing, 26
notes, 27
sense wires, 48
siren
connecting, 49
in workflow, 21
Smart Power Switch
in workflow, 20
installing, 41
power cable
in workflow, 22
installing, 42
SPS
in workflow, 20
installing, 41
switch
PoE
in workflow, 20
installing, 33
Smart Power
in workflow, 20
installing, 41
system power cable
in workflow, 21
installing, 50

T

testing
in workflow, 22
installation, 52
through-hole antenna, 37
tools list, 13
torch method, 23
training information, 6
triggers
auxiliary, 49
brakes, 49
connecting, 48
emergency lights, 49
ignition, 49
in workflow, 21
radar interface, 50
siren, 49

U

upload, cellular, 55
USB dongle LTE modem, 55

V

V300 antenna
in workflow, 21
installing, 44
V300 kit, 12
V300 system, 40
V300 WiFi Base
in workflow, 21
installing, 44
verifying installation, 52
in workflow, 22
Vigilant cameras, 56
VISTA WiFi antenna
in workflow, 21
installing, 44
VISTA WiFi Base
in workflow, 21
installing, 44
VISTA WiFi kit, 11
VISTA WiFi system, 40
VISTA XLT system, 40

W

WiFi Base
in workflow, 21
installing, 44
wireless microphone
in workflow, 21
installing, 45
wireless microphone antenna
in workflow, 21
mounting, 15, 45
wireless radio
configuring, 35

Groove, 39
in workflow, 20
installing, 36
types, 35
wireless radio antenna
in workflow, 20
mounting, 36
wires
auxiliary, 49
black with white stripe, 49
blue with white stripe, 49
brakes input, 49
emergency lights, 49
ignition, 49
orange and brown, 49
pink and green, 49
power and ground, inputs cable, 49
purple/black/gray connector, 50
radar interface connector, 50
siren, 49
solid blue, 49
triggers, 48
white, 49
workflow, full install, 19

Z

Zero Sightline camera, 25
ZSL camera, 25

This page intentionally left blank.

YARMOUTH POLICE DEPARTMENT
POLICY AND PROCEDURE

AUTOMATIC LICENSE PLATE RECOGNITION (ALPR)
2019-10

Date of Issue: 11/22/2019 Review Date : Revised:	Issuing Authority:  Chief Frank G. Frederickson
Certification Standards: Accreditation Standards: Optional Accreditation Standards:	

Purpose

The purpose of this policy is to establish guidelines and procedures for the proper use and application of the Automatic License Plate Recognition (ALPR) System.

Policy

The availability and use of the ALPR System provides opportunities for the enhancement of law enforcement agencies' productivity, effectiveness, and protection of public and officer safety. The Yarmouth Police Department shall only utilize the technology in furtherance of official and legitimate law enforcement operations and public safety. All department employees shall abide by the guidelines set forth herein when using the ALPR System.

Definitions

Automatic License Plate Recognition (ALPR): Automatic license plate recognition technology uses high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The ALPR System captures an image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to the CJIS-NCIC Hot file database. The ALPR System is configured as either fixed, mobile or portable.

Alert: A visual and/or auditory notice that is triggered when the ALPR System receives a potential hit on a license plate.

Alert Data: Information captured by an ALPR relating to a license plate that matches the license plate on a hot list.

ALPR Data: Scan files, alert data, and any other documents or data generated by, or obtained thorough, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

Hit: An alert that a license plate matches a record maintained in the ALPR database related to stolen vehicles, wanted vehicles, or other alert type files that support investigation or which have been manually registered by a user for further investigation.

Hot List: License plate numbers of vehicles of interest, such as stolen vehicles, unregistered vehicles, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Silver Alerts, Be On Look Out (BOLO), Attempt To Locate (ATL), and Wanted or Missing Person broadcasts or bulletins in which a license plate number is included, or other license plate numbers of interest entered by the Department or an authorized officer.

Hot List Download: The method by which the hot list data is transferred to a computer within a law enforcement vehicle.

Optical Character Recognition (OCR): The technology that supports the automated reading and digitizing of images of license plates that are captured by the ALPR System.

ALPR Administrator

The Detective Sergeant and the Lieutenant in Charge of Detectives shall be designated as the ALPR Administrators.

The ALPR Administrator shall be responsible for the following:

- Ensuring that only authorized personnel have access to the ALPR system
- Authorizing requests for *Hot List* search
- Ensuring that designated, trained personnel check equipment on a regular basis to ensure functionality, camera alignment, and removing from service any equipment that falls outside expected functionality until deficiencies are corrected.

The ALPR Administrator shall:

1. Designate users who have been properly trained in the use and operational protocols of the ALPR System;
2. Allow access to the ALPR System for those users with an approved login and password; and
3. Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

ALPR Procedures

Use of the ALPR technology shall be limited to the authorized members of the Yarmouth Police Detective Division.

ALPR System and information shall be:

- Accessed and used only for official and legitimate law enforcement purposes;
- Used for searches of historical ALPR data, in accordance with this policy and other Department policies or regulations where applicable; and
- Used for searches of ALPR data by other law enforcement agencies through the ALPR Administrator.
- Emergency access to ALPR data can be accomplished through a request from the on-call detective.

Manual Entry of Data/Manual Hot List

Manual entries may only be entered by the ALPR Administrator.

Manual entries may include, but should not be limited to:

- AMBER Alerts;
- Missing Child Alerts;
- Missing College Student Bulletins;
- Silver Alerts;
- Be On Look Out (BOLO);
- Attempt To Locate (ATL); or
- Wanted or Missing Person broadcast or bulletin in which a license plate number is included.

Manual entries entered into the ALPR System shall be:

- Manually updated when the information changes or is no longer current;
- Documented with the specific reason by the member:
- Documented with agency case number; and
- Given a retention date of 1 year or less.

Patrol Access

The Yarmouth Police Detective Division can be contacted through our normal on-call procedures for emergency access to the ALPR data.

Any mention of the plate reader or information request on the radio should be avoided in order to maintain the integrity of the program.

ALPR Data: Logs, Sharing Dissemination and Retention

The following process shall apply to ALPR Data:

- A Query Log is internally maintained by each instrument for each transaction;

- Data can be accessed, retrieved, or shared for official and legitimate law enforcement business only; and
- Retention of data shall be determined by the Department of Criminal Justice Information Services (DCJIS) Policy.

Policy Review

The ALPR Administrator shall be responsible for:

- Annual review of this policy and the procedures contained herein; and
- Making recommendations to the Chief or designee, for any amendments

As use of the technology progresses, the department shall continue to monitor and assess the appropriateness of this policy, as new technology may raise both legal and technological issues.

Department of State Police
DIVISION COMMANDER'S ORDER

Issue Date	**Number**
May 3, 2022	**2022-DHS-002**
Subject: **Use of Non-Departmental ALPR Systems**	

The Division of Homeland Security and Preparedness is responsible for the administration of the Department's Automatic License Plate Recognition System (ALPR). The availability and use of ALPR technology provides opportunities to increase public and officer safety and to enhance the effectiveness of law enforcement agencies.

The Department shall only utilize ALPR technology in furtherance of official and legitimate law enforcement operations and public safety. The use of ALPR technology is governed by General Order TRF-11 "Automatic License Plate Recognition". In addition, the use of non-departmental ALPR systems shall be subject to the guidelines set forth in this Order until and unless superseded by General Order TRF-11.

In the course of their official duties, members may contact other law enforcement agencies to request assistance with information, records, or data from non-departmental ALPR systems.

Lieutenants and supervisory analysts assigned to the Commonwealth Watch Center/Commonwealth Fusion Center and the ALPR Administrator may access accounts with non-departmental ALPR systems for official law enforcement purposes as authorized by General Order TRF-11.

Other members, through their position with the Department, shall not obtain accounts with non-departmental ALPR systems unless authorized by the Division Commander of the Division of Homeland Security and Preparedness.

Members shall be mindful that non-departmental ALPR systems may use different technology and quality assurance standards than the Department's ALPR system.

_____

Christopher T. Wilcox
Lieutenant Colonel
Division of Homeland Security and Preparedness

Department of State Police
General Order

Effective Date:	Number:
_____, 2022	TRF-11
Subject:	
Automatic License Plate Recognition	

Policy

The availability and use of Automatic License Plate Recognition (ALPR) technology provides opportunities to increase public and officer safety and to enhance the effectiveness of law enforcement agencies. The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

The Department shall only utilize ALPR technology in furtherance of official and legitimate law enforcement operations and public safety. All Department employees shall abide by the guidelines set forth herein when using ALPR systems.

Purpose

To establish guidelines and procedures for the proper use and application of ALPR technology within the Department of State Police, and to provide guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information to ensure that this information is used only for legitimate law enforcement purposes and the privacy, civil rights, and civil liberties of individuals are not violated.

Definitions and Acronyms

Alert: A visual and/or auditory notice that is triggered when the ALPR system receives a potential hit on a license plate.

ALPR Data: Data generated by ALPR devices, including the license plates observed by the ALPR device, the date and time of reads, the ALPR device that sourced the reads, and related data.

Automatic License Plate Recognition (ALPR): Automatic license plate recognition (also commonly referred to as automated license plate reader) technology uses cameras to capture images of license plates and computer algorithms such as Optical Character Recognition (OCR) to convert the images to readable text data. ALPR systems can also compare the recognized license plates to Hot Lists such as Criminal Justice Information System (CJIS) and National Crime Information Center (NCIC) Hot File databases.

Exigent Circumstances: Emergency situations involving imminent and immediate threat to the safety, health, and well-being of an individual or the public based on specific, reasonable intelligence. Such emergency situations shall include, but are not limited to, terrorist threats, Amber Alerts, Silver Alerts, kidnappings, missing persons, and felons traveling to or from a crime scene.

Definitions and Acronyms, continued

Hit: A match between a license plate observed by an ALPR camera and a record maintained on a Hot List.

Hot List: A list of license plate numbers, including stolen vehicles and plates entered into CJIS/NCIC as well as missing persons, Amber & Silver alerts associated with a vehicle registration, wanted criminals, and others of specific interest to law enforcement that have a vehicle or tag associated to them. This may also include vehicles which are the subject of ongoing public safety or criminal investigations that are entered by the Department or an authorized officer.

Non-Departmental ALPR Systems: ALPR systems which are not run, managed, or subscribed to by the Department and include ALPR systems in use by other law enforcement agencies.

Optical Character Recognition (OCR): The technology that supports the automated reading and digitizing of images of license plates that are captured by the ALPR System.

Authorized Uses

This policy is provided to support authorized uses of ALPR information. Authorized uses shall include the following:

- Enhance the Department's AMBER/SILVER and other law enforcement alerts programs, situation awareness, and real-time response capability by deploying ALPRs to more rapidly identify and locate vehicles related to potential child abductions, kidnappings, missing persons, or other emergency situations or serious crimes;
- Support the Department's homeland security mission through the investigation, prosecution, and prevention of suspected terrorist incidents and the protection of critical infrastructure and locations that allow for travel and the free flow of commerce from subjects who intend to damage or disrupt the systems;
- Support law enforcement response to critical incidents and the protection of high-profile public events which may be a potential target of a terrorist attack or mass-casualty incident;
- Protect the safety of the motoring public and alert law enforcement in real-time that a particular license plate (e.g., a stolen vehicle or a vehicle associated with a wanted individual) is in close proximity to an ALPR to dramatically reduce the recovery time of stolen vehicles, aid in the removal of unsafe vehicles from the roadway, and assist in locating dangerous and wanted individuals;
- Support the Department's public safety mission through the investigation and prosecution of suspected criminal (including terrorist) incidents;
- ~~The follow-up investigation of motor vehicle pursuits which have been terminated for public safety reasons or when an unlawfully fleeing subject escaped apprehension;~~
- Support local, state, federal, and tribal public safety agencies through the use of ALPR technology as allowed by this policy; and
- Support other lawful Department public safety operations, as directed by the Colonel/Superintendent or designee.

Prohibited Uses

The Department will prohibit access, use, or dissemination of ALPR information for:

- Any purpose that violates the Constitutions or laws of the United States or the Commonwealth of Massachusetts, including the protections of the Fourth Amendment;
- Based solely on an individual's or organization's religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law;
- Non-law enforcement or personal purposes;
- The purpose of prohibiting, infringing upon, or deterring individual activities protected by the First Amendment, such as freely practicing one's religion, freedom of speech and peaceful assembly, freedom of the press, and the right to petition the government for the redress of grievances;
- Harassing, targeting, and/or intimidating any individual or group by means of camera placement or data use in a discriminatory manner;
- The sole purpose of locating or removing persons due to their citizenship or immigration status; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

ALPR Administrator

The Division Commander of the Division of Homeland Security and Preparedness (DHS) shall:

- Designate a Commissioned or Non-Commissioned Officer as the ALPR Administrator; and
- Ensure the ALPR Administrator has oversight for the ALPR System deployment, operations, and maintenance.

The ALPR Administrator shall:

- Manage access to the ALPR system and designate personnel who have been trained in the use and operational protocols of the ALPR system;
- Coordinate with all Divisions to ensure resources are available and deployed to meet Departmental needs;
- Maintain proficiency and familiarity with ALPR systems, coordinate with other law enforcement agencies, and assist with investigations involving ALPR systems;
- Ensure that ALPR equipment is checked on a regular basis to ensure functionality, and remove from service any equipment that falls outside expected functionality until deficiencies are corrected;
- Conduct testing and evaluation of ALPR systems and make recommendations to the Department regarding the purchase or use of ALPR systems and equipment;
- Coordinate the purchase, deployment, and installation of ALPR equipment;
- Conduct intermittent audits of ALPR system usage to ensure functionality and policy compliance; and
- Ensure that any changes in policy or law are the subject of continuing in-service training or bulletins.

Search Procedures

The Commonwealth Watch Center (CWC) and Commonwealth Fusion Center (CFC) shall serve as the primary ALPR resources for officers that are not designated ALPR system users.

Searches of ALPR data shall be conducted in accordance with this policy and other Department policies or regulations where applicable.

Searches of the ALPR system shall observe the following guidelines:

- Enter justification categories at the time of the search;
- Limit searches to the geographic area that is reasonable and consistent with the needs of the incident or investigation;
- Limit searches to a time period of thirty (30) days or less, except under the following circumstances:
  - Justified by exigent circumstances;
  - Target license plate is associated by specific and articulable facts with the subject of an arrest warrant or warrant of apprehension;
  - Where there has been a significant delay in reporting the offense to be investigated; new information or evidence has become available; or the investigation is being conducted diligently and expeditiously and is not yet completed;
  - As authorized by a court order or search warrant.
- Document the parameters used during the search if applicable during a criminal investigation.

Manual Hot List Entries

Manual entries of a license plate onto a Hot List may include vehicles associated with:

- AMBER or Silver Alerts;
- Missing child alerts;
- Missing college student bulletins;
- Incapacitated or endangered Persons;
- Be-On-Look-Out (BOLO) or Attempt To Locate (ATL);
- Investigation of terrorist or criminal incidents;
- Wanted persons, arrest warrants, or search warrants; or
- Missing person or kidnapping broadcasts or bulletins.

Manual entries onto a Hot List shall be:

- Entered by the CWC/CFC or a designated user;
- Approved by a supervisor, except in exigent circumstances;
- Entered with the vehicle description, if available;
- Entered with a case number, if available;
- Updated or removed when information changes or is no longer current, with special attention given to rental and other short-term use vehicles;
- Removed as soon as appropriate for the investigation; and
- Given an initial expiration date of thirty (30) days or less.

Mobile Operations

Department cruisers may be affixed with a mobile ALPR system which provides hit/alert information via a mobile data terminal in the cruiser. Members operating a cruiser that is equipped with a mobile ALPR System shall:

- Ensure, at the start of each shift or upon activation of the ALPR system, that the ALPR system has been updated with the most current hot lists available;
- Verify, prior to use, the aim of the ALPR camera(s) to ensure it is focused on the correct lanes of traffic;
- Ensure ALPR equipment is cleaned and maintained according to the manufacturer's recommendations; and
- Notify the ALPR Administrator of any malfunctions promptly.

Hit/Alert Confirmation

An ALPR hit or alert shall not form the basis for a motor vehicle stop or enforcement action until and unless it is confirmed. Prior to initiation of a stop or enforcement action based upon an ALPR hit or alert, members shall confirm the hit or alert, including:

- *Verify the plate:* Visually verify that the vehicle plate matches the ALPR system's OCR interpretation;
- *Verify the state:* Visually verify that the state of the vehicle plate matches the state of the plate in the Hot List information; and
- *Verify the status:* Verify the current status of the plate (e.g., is the vehicle still stolen or the subject still wanted?), through:
    - Criminal Justice Information System(CJIS);
    - National Crime Information Center (NCIC);
    - Department's Records Management System (RMS); or
    - Another appropriate source of data.

Use of Non-Departmental ALPR Systems

In the course of their official duties, members may contact other law enforcement agencies to request assistance with non-departmental ALPR information. Members, through their position with the Department, shall not obtain personal access or accounts with non-departmental ALPR systems unless authorized herein or by the Division Commander of the Division of Homeland Security and Preparedness.

The Commonwealth Watch Center and Commonwealth Fusion Center, the ALPR Administrator, and members of task forces or specialized assignments where ALPR systems are used for official duties may access non-departmental ALPR systems for official law enforcement purposes as authorized within this policy, and/or in compliance with the policy or procedures of the task force or specialized assignment to which the member is assigned.

Members shall be mindful that non-departmental ALPR systems may use different technology and quality assurance standards than the Department's ALPR system. Additional steps may be necessary to verify the accuracy of data obtained from outside ALPR systems prior to use in an enforcement action or investigation.

Requests for the deployment of ALPR equipment pursuant to operational needs shall be directed to the ALPR Administator. Requests for mobile ALPR equipment on a Department vehicle shall be submitted through channels to the member's Troop/Section/Unit Commander, who upon approval shall forward the request to the ALPR Administrator.

Requests for ALPR Equipment or Accounts

Requests for access to the Department's ALPR system shall be directed through the member's Troop/Section/Unit Commander to the ALPR Administrator. Requests for access to a non-departmental ALPR system shall be directed through the member's Troop/Section/Unit Commander to the ALPR Administrator and the Division Commander of the Division of Homeland Security and Preparedness.

The ALPR administrator will approve, deny, or forward requests for deployment, equipment, and accounts as authorized under this policy and based upon the statewide needs of the ALPR program and the availability of suitable equipment and personnel.

Data: Sharing, Retention, and Discovery

License plate numbers and date/time location records collected through an ALPR do not identify the individual operating or associated with a vehicle. Investigators may be able to link an individual to a vehicle through, or in combination with, additional information from other sources, such as a check of vehicle registration records. It is thus the investigative process that may identify individuals and not solely a reliance on the information obtained from the ALPR system's automated observation of license plate characters. The Department protects all ALPR information as personally identifiable information (PII) because ALPR information may be combined with other information to identify a unique individual.

The Department and members shall not share ALPR data with or provide ALPR data to any person, entity, or agency, other than a law enforcement agency with an originating agency identifier (ORI), unless such disclosure is authorized by law or court order or is required by rules of Massachusetts or federal courts governing discovery in criminal matters.

Data contained in the ALPR system may include data contributed by other law enforcement agencies. Agencies and their members that are authorized to share data with the Department or access the Department's ALPR data shall be subject to the provisions of this policy in regards to use of the Department's ALPR system. However, such agencies are responsible for their own designation, management, and supervision of system users and equipment.

The Department's ALPR system shall retain ALPR data that has not been linked to a case or investigation for no longer than sixty (60) days OR ninety (90) days. Members using the ALPR system are responsible for preserving, exporting, or obtaining copies of relevant records or reports prior to the expiry of the records. Failure to properly export records or reports in a timely manner may result in the loss of evidence.

Data: Quality Assurance

Original ALPR information will not be altered, changed, or modified in order to protect the integrity of the data. Any changes will be maintained as a separate and additional record, and such record will be identified as having been modified.

The Department will correct, notate, delete, or refrain from using ALPR information the Department originated and found to be erroneous or deficient. Originating agencies external to the Department are responsible for reviewing the quality and accuracy of the ALPR information provided to the Department and must take reasonable steps to correct or amend the information upon learning that it is inaccurate or deficient. The Department will advise the appropriate points of contact, in writing or electronically, if the Department's ALPR information is found to be erroneous or deficient.

The Department will ensure that appropriate protocols are utilized by the ALPR system to allow for the verification of the accuracy of ALPR read times, which may include the use of a watermark or other observable system indicator. In the event that system time is not verifiably synchronized for a particular read, the reported time should be corroborated using other data or observations to ensure accuracy prior to use in an investigation.

Data: Security & Audit

The following shall apply to ALPR system and information security:

- Access to the Department's ALPR system will be granted only to personnel whose positions and job duties justify such access, who have successfully completed a pre-employment background check, and who have completed appropriate training;
- Usernames and passwords to the ALPR system are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR system will be logged into the system identifying the user initiating the query. All user access and queries, including participating agencies access, are subject to review and audit;
- Abuse of the Department's ALPR system may result in termination of system access and progressive discipline; and
- The Department will ensure that ALPR data is stored in a secure manner, on CJIS-compliant systems or servers, in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions.

Policy Review

Existing technology may progress and new technology may develop, giving rise to both legal and technological changes. The Department will monitor and assess the appropriateness of this policy and make amendments as necessary.

The ALPR Administrator shall:

- Annually review this General Order and the procedures contained herein; and
- Make recommendations for any necessary amendments through channels to the Colonel/Superintendent or designee.

References: Commonwealth vs. McCarthy, 484 Mass. 493
Denise Green v. City and County of San Francisco, 751 F.3d 1039
United States v. Knotts, 460 U.S. 276
United States v. Wilcox, 415 F. App'x 990
United States v. Yang, 958 F.3d 851
700 CMR 7.00

Promulgated By: Christopher S. Mason, Colonel/Superintendent

boss4

Home › Groups

Groups

- Massachusetts Host
- Methuen PD
- Interagency
- Barnstable PD
- Dennis PD
- Taunton PD
- Yarmouth PD
- Raynham PD
- Seekonk PD
- Attleboro PD
- Regional Hotlist Groups
- MSP Mobile Systems
- MSP Dispatch

GROUPS — Add a new group

Type a name for the group

Description

USERS

Select the users for this group

ROLE

Select the role for this group

HOTLISTS

Select the hotlists for this group

ACCESIBLE REPORTS

Select the reports for this group

Enforce historical search limit

Maximum search days: 30

CANCEL SAVE

Commonwealth of Massachusetts

Office of the Middlesex District Attorney

Appeals & Training Bureau

2022-2023 POLICE TRAINING MANUAL

UPDATED THROUGH SEPTEMBER 30, 2022

receive the responsive records. In most cases, that contact is the affiant; therefore, the warrant should list the police department, contact name, address, phone & fax number, along with an email address to which the provider can send the requested records.

Because the fourteen-day period statutorily provided for production of the requested records (along with "an affidavit from the person in custody of those records certifying that they are true and complete") is longer than the seven-day return period for a search warrant, the Middlesex District Attorney's Office offers the following as sample language for the search warrant return:

> On [DATE], I, Officer [NAME] of the _____ Police Dept., served warrant no. _____ upon [CORPORATION] at [ADDRESS] by [WHAT MEANS (mail/fax/delivery service)]. It is expected that [CORPORATION] will transmit the records authorized by the warrant to local law enforcement officers in compliance with G.L. c. 276, § 1B. Copies of all such records produced pursuant to the warrant will be provided to the defense in the pretrial discovery process.

The service and return process for search warrants applies generally to all companies that provide electronic communication or remote computing services, including cell phone companies. Note that, pursuant to G.L. c. 276, § 1B, search warrants seeking records from such companies can be served via fax or email regardless of where the headquarters are located.

VIII. DIGITAL SURVEILLANCE TECHNOLOGY & THE MOSAIC THEORY

In recent years, technological developments have resulted in the proliferation, increased ease of use, and affordability of numerous surveillance tools. See Commonwealth v. Perry, 489 Mass. 436, 444 (2022) ("advancements in technology have resulted in a quantity and quality of surveillance that never could have been imagined, let alone realized, at the time of the founding"). Law enforcement's access to these "extraordinarily powerful" surveillance tools has prompted the Supreme Judicial Court and the United States Supreme Court "to guard against the 'power of technology to shrink the realm of guaranteed privacy[.]'" Commonwealth v. McCarthy, 484 Mass. 493, 498 (2020), quoting Commonwealth v. Almonor, 482 Mass. 35, 41 (2019). In Massachusetts, this response has taken the form of the adoption of the "mosaic theory" to

determine whether electronic surveillance intrudes upon a reasonable expectation of privacy such that a warrant is required (or an exception thereto).

The mosaic theory is an "aggregation principle for the technological surveillance of public conduct" grounded in the recognition of an individual's "privacy interest in the whole of one's public movements." McCarthy, 484 Mass. at 502, 503. See also Commonwealth v. Henley, 488 Mass. 95, 108-114 (2021); Commonwealth v. Mora, 485 Mass. 360, 368 (2020). The theory recognizes that while a person's isolated movements in public are not typically a subject of constitutional protection, when viewed in the aggregate over a prolonged period of time, such detailed location data can encroach upon a person's reasonable expectation of privacy. McCarthy, 484 Mass. at 504, 508. See also Katz v. United States, 389 U.S. 347, 351 (1967) ("the whole of one's movements, even if they are all individually public, are not knowingly exposed in the aggregate"); Commonwealth v. Connolly, 454 Mass. 808, 833-834 (2009) (Gants, J., concurring) (aggregated location data reveals "a highly detailed profile, not simply of where we go, but by easy inference, of our associations – political, religious, amicable and amorous, to name only a few – and of the pattern of our professional and avocational pursuits"). "[R]ather than 'asking if a particular act is a search, the mosaic theory asks whether a series of acts that may not be searches in isolation amount to a search when considered as a group.'" Perry, 489 Mass. at 445, quoting Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012).

The mosaic theory is a totality of the circumstances test, looking to several factors in an attempt to discern whether electronic surveillance (which includes the search of digital evidence such as CSLI) "was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life." Id., quoting Mora, 485 Mass. at 373. These factors include the duration and degree of comprehensiveness of the surveillance, the extent to which the surveillance tends to reveal highly intimate or personal details, and whether the electronic surveillance generated a category or quantity of information that could not have been obtained using traditional law enforcement surveillance. Perry, 489 Mass. at 445-449. In considering this last factor, courts pay particular attention to the ability of law enforcement to reconstruct past movements, as well as the degree to which the comparable traditional

surveillance method would have been prohibitively expensive or impractical. Id. at 449. However, "these factors are not exhaustive, and no one factor is determinative." Id.

In creating a vague, multi-factor test and refusing to draw bright-line rules with respect to different surveillance technologies, the SJC has put the onus on law enforcement to determine when electronic surveillance crosses the threshold into an impermissible search that infringes on an individual's reasonable expectation of privacy. See, e.g., Mora, 485 Mass. at 376; McCarthy, 484 Mass. at 509 n.15 ("In declining to establish a bright-line rule for when the use of ALPRs constitutes a search, we recognize this may bring some interim confusion"). As demonstrated infra, the court has provided some guidance with respect to certain technologies. However, the analysis will inherently be fact-specific, and the Middlesex District Attorney's Office recommends consulting with an Assistant District Attorney before determining whether to proceed with or without a warrant.

A. Automatic License Plate Readers (ALPR's)

In McCarthy, 484 Mass. at 508-509, the first case to address and adopt the mosaic theory, the SJC held that police did not intrude on a defendant's reasonable expectation of privacy where they used information obtained from four ALPR's in fixed positions on either side of two bridges to determine when, over a period of three months, a defendant crossed the bridges. While recognizing that ALPR's provided police with surveillance capabilities that exceeded what would have been possible using traditional law enforcement techniques, the court reasoned that the limited number of ALPR's, positioned on public highways leading to and from the Cape Cod peninsula, did not "allow the Commonwealth to monitor the whole of the defendant's public movements" or otherwise "reveal 'the privacies of life.'" McCarthy, 484 Mass. at 508-509, quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

The court was clear, however, that a broader network of cameras capturing additional details about a defendant's movements would trigger the warrant requirement, particularly where the system in question retains historical data for a prolonged period, allowing authorities to reconstruct past movements. See McCarthy, 484 Mass. at 506 ("A network of ALPR's that surveils every residential side street paints a much more nuanced and invasive picture of a driver's life and public movements than one limited to major

highways that open into innumerable possible destinations"). The court also cautioned that even a limited number of ALPR's located near "constitutionally sensitive locations," such as the home or a place of worship, could intrude upon one's reasonable expectation of privacy because they "reveal more of an individual's life and associations." Id. at 506. Thus, for example, it is likely that a network of cameras stationed at tollbooths tracking the defendant's movements from Worcester to downtown Boston and back around the time of a suspected crime would implicate the mosaic theory. The same outcome is likely if a network of traffic cameras in a particular city or town tracked a suspect's specific movements through the city throughout the course of week or even (perhaps) a day. The McCarthy court was clear that "the amount of data that the government collects or to which it gains access" is the relevant barometer for whether a particular form of electronic surveillance implicates a mosaic. 484 Mass. at 505-506 ("our constitutional analysis ideally would consider every ALPR record of a defendant's vehicle that had been stored and collected by the government up to the time of the defendant's arrest"). Thus, in crafting requests for ALPR's, particularly when dealing with larger networks of cameras, authorities should specifically set forth particular areas or particular cameras of interest.

B. Pole Cameras

The SJC next turned its attention to pole camera surveillance, an investigatory tool that had, for decades, evaded art. 14 scrutiny. In Commonwealth v. Mora, 485 Mass. 360 (2020), the court addressed whether prolonged pole camera surveillance targeting a suspect's residence amounted to a constitutional search under art 14. Concluding that targeted long-term pole camera surveillance "has the capacity to invade the security of the home," an area traditionally entitled to heightened constitutional protection, the SJC held that the duration in question – a period of two months – required a warrant. See Mora, 485 Mass. at 371-372 ("even when pole cameras do not see into the home itself, by tracking who comes and goes over long periods of time, investigators are able to infer who is in the home, and with whom the residents of the home meet, when, and for how long"). The SJC subsequently narrowed this period to roughly two weeks. See Commonwealth v. Comenzo, 489 Mass. 155, 160 n.9 (2022) (pole camera monitoring residence for period of thirteen days amounted to search under art. 14). Crucially, the

ALPR BRIEFING

February 2022

U//LES - Do Not Disseminate

Disclaimer and Warning

- This presentation contains **law enforcement sensitive** information that could compromise public safety and critical infrastructure if disseminated or released.
- This presentation includes discussion of the Department's potential future use of technology, expenditure of funds, and revisions to policy and procedure.
- Any talking points or suggestions contained herein are intended to facilitate discussion and are not intended to represent the official position or future direction of the Department.

U//LES - Do Not Disseminate

Mission Statement

- Provide intelligence-based infrastructure, accessible software, real-time support and assistance, and mission-focused training to allow law enforcement investigative units to utilize automated license plate recognition technology in a lawful manner to protect the citizens of the Commonwealth of Massachusetts.

U//LES - Do Not Disseminate

Topics to be Covered

- State of MSP ALPR program
  - Software, hardware, and system transition
- State of ALPR technology & industry
- Policy and practice review
- Future & goals of MSP program

U//LES - Do Not Disseminate

State of the Program

U//LES - Do Not Disseminate

ALPR Configurations

Department employs ALPR in four (4) configurations:

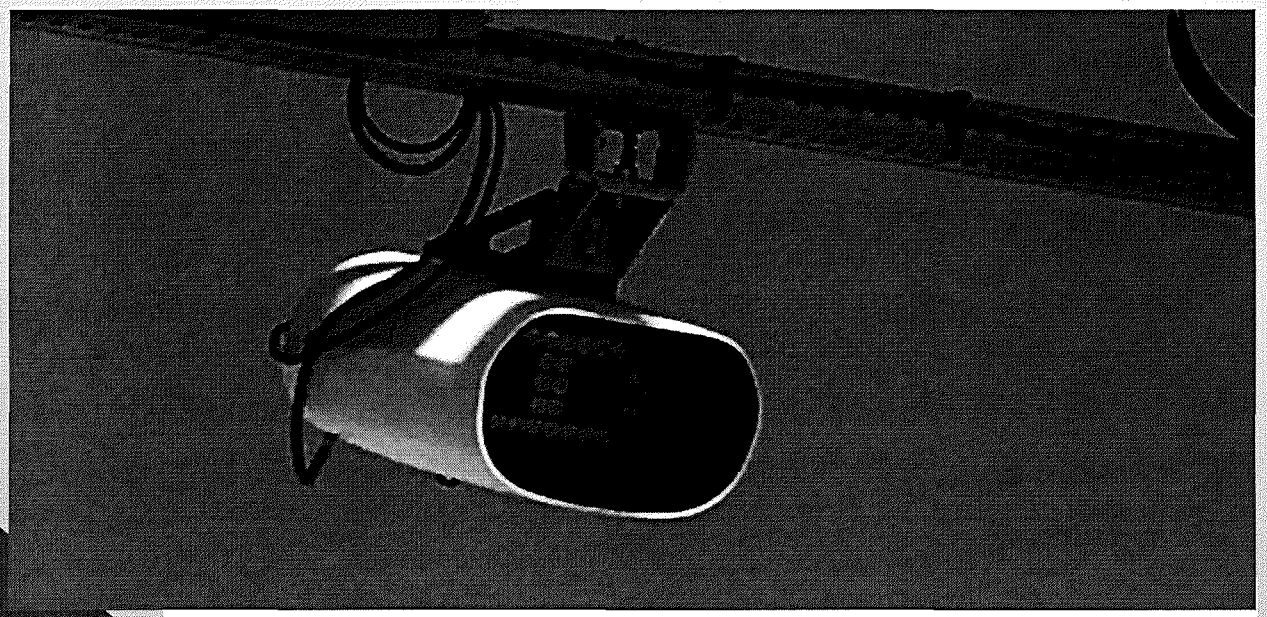
- **Fixed Overt**
- **Fixed Covert**
- **Trailers**
- **Mobile**

We will review each one in greater detail.

U//LES - Do Not Disseminate

Fixed Overt

- Fixed overt sites are hard-wired at critical infrastructure locations:
  - G.L. c. 4.sec. 7.cl.26 (n)(security)
  - [redacted]



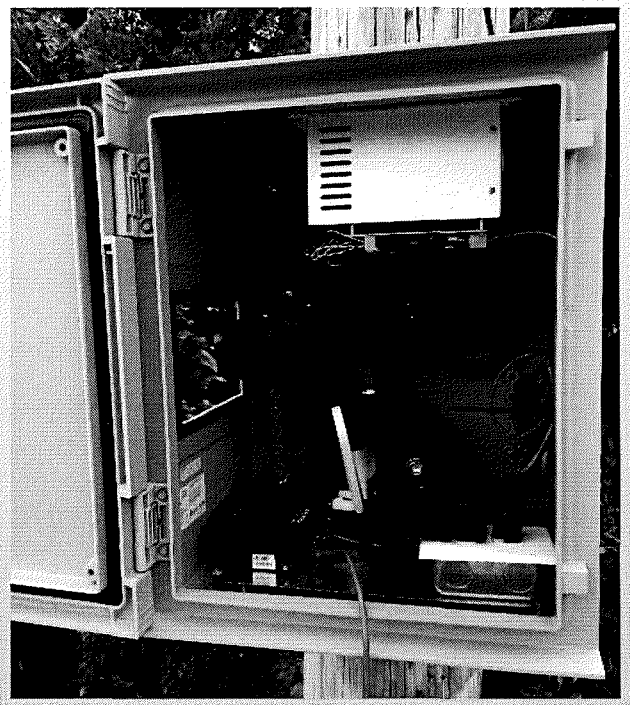
U//LES - Do Not Disseminate

Fixed Covert

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

- Department owns approximately G.L. c. 4.sec. 7.cl.26 (n)(security)
- Department hosts G.L. c. 4.sec. 7.cl.26 (n)(security) for local partners, with G.L. c. 4.sec. 7.cl.26 (n)(security) awaiting installation

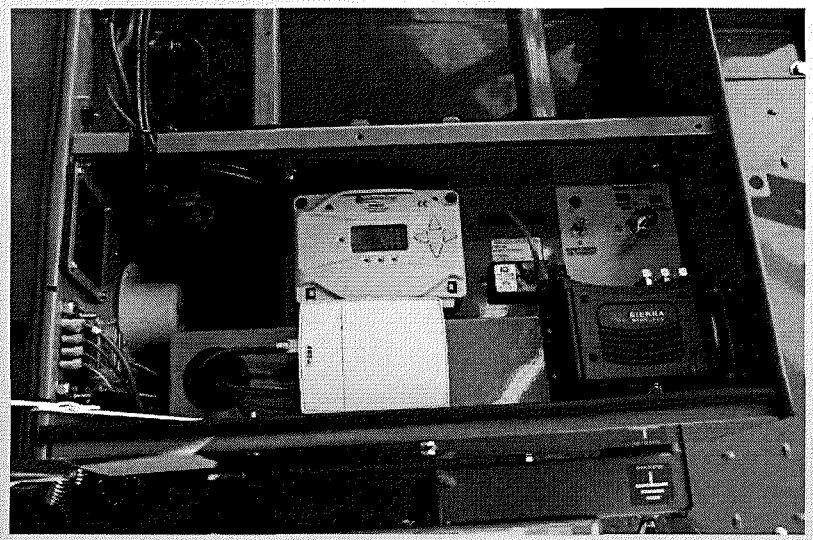


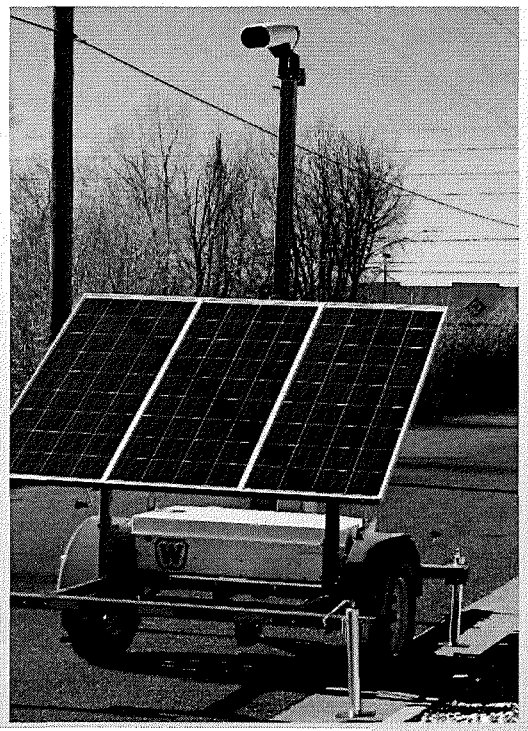


U//LES - Do Not Disseminate

Trailers

- Cameras, modems, and hardware are installed on solar powered trailers, which can be deployed and relocated as needed
- Fleet [G.L. c. 4.sec. 7.cl.26 (n)] trailers, [G.L. c. 4.sec. 7.cl.26 (n)(security)] deployed, remainder at [G.L. c. 4.sec. 7.cl.26 (n)(security)])
- Recalled in winter due to poor solar performance and risk of damage from snowplows

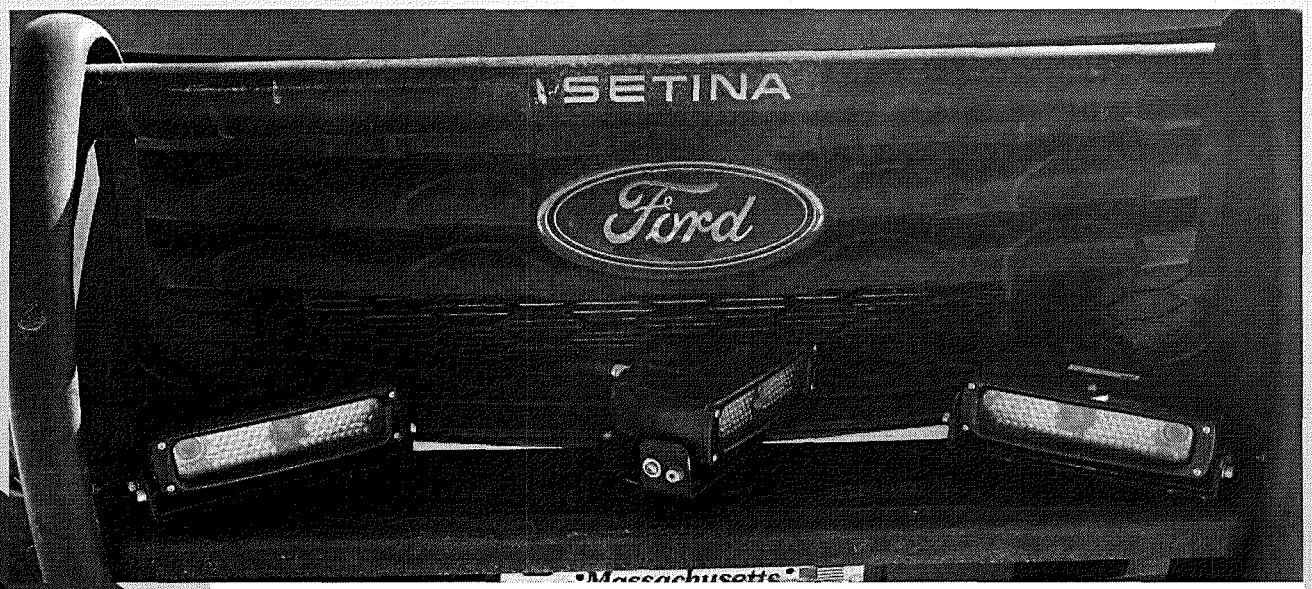




U//LES - Do Not Disseminate

Mobile: Cruiser Mounted

- Mobile cameras are mounted to cruiser roof or push bumper
- Deployed on DFS cruisers, mostly CVES
- Existing mobile units (approximately 20) are OOS or not recording to system database, and most cannot be upgraded due to age
- New mobile units (26) have been ordered from a CVES grant



U//LES - Do Not Disseminate

Department Equipment Summary

Summary of Department Owned Equipment:

- **Fixed Ove** G.L. c. 4.sec. 7.cl.26 (n)(security)
- **Fixed Cov**
- **Trailers:**
- **Mobiles:**

Totals:

- Cameras, working or available:
- Cameras, currently online:
- Cameras, broken or OOS (exc. mobile):
- Available data plans:

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

U//LES - Do Not Disseminate

Interagency Equipment Summary

Department has offered the service of hosting ALPR data for partner agencies

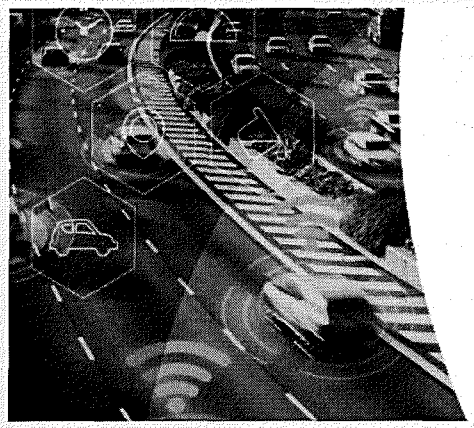
- Agencies purchase their own equipment and register it to our system
- Makes the technology accessible to local partners at reasonable cost
- Facilitates reliable data management and interagency cooperation
- An MOU has been drafted and is under review by MSP Legal Section

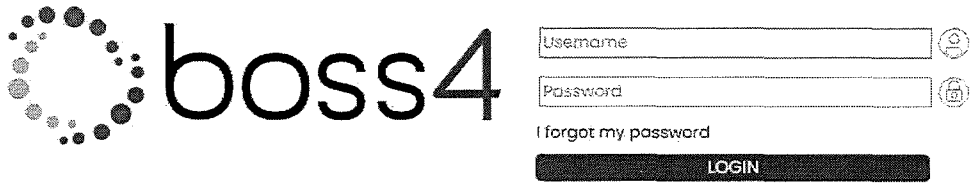
Summary of Hosted Equipment:

- **Fixed:** [redacted] cameras for 3 agencies (1 additional pending install)
- **Mobiles:** [redacted] to system database (approx. 13 agencies were active)

U//LES - Do Not Disseminate

ALPR Software

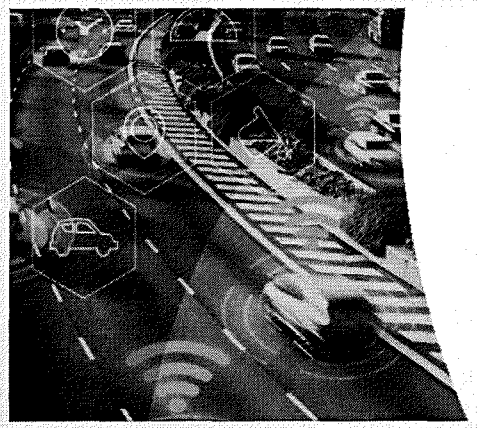


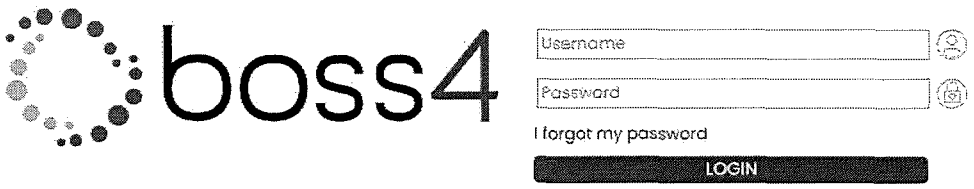


- Transition in progress to new ALPR software: **Neology Boss4**
- Legacy system used server at DCJIS and required local software
- New system is hosted in AWS government cloud and web-based
- Funding for upgrade (approx. $500,000 for three years of service) was provided by EOTSS in exchange for removing server

U//LES - Do Not Disseminate

ALPR Software





- Software development is ongoing, and inadequacies that affect usability are being addressed directly with the vendor
- Upgrades are expected to be batched by quarter and released over 2022
- Access the **Boss4** website is currently blocked by EOTSS, rendering it inaccessible from within the MSP network; negotiations are ongoing to resolve

U//LES - Do Not Disseminate

Boss4 Transition:
Status & Timeline

Status: ***in progress***

- Migrating sites one by one, identifying and fixing issues along the way

Timeline:

- Completed so far:
  - G.L. c. 4.sec. 7.cl.26 (n)(security)
  - [redacted]
  - [redacted]

U//LES - Do Not Disseminate

Boss4 Transition:
Status & Timeline

Timeline:

- February 2022:
  - Boss4 website access allowed by EOTSS
  - Remaining fixed overt sites switched G.L. c. 4.sec. 7.cl.26 (n)(security)
  - Watch Center online & trained to handle requests in both systems
- March 2022:
  - Trailer fleet at Fort Devens completed and available
  - Department's fixed covert sites 50% completed
  - Hosted local PD mobile tenants started (pending MOU approval)
  - Highest priority Boss4 software upgrades completed by vendor (Q1)

U//LES - Do Not Disseminate

Boss4 Transition:
Status & Timeline

Timeline:

- April 2022:
  - Department's fixed covert sites completed
  - Hosted local PD fixed sites completed
  - Receive new CVES mobile units and begin installations
- May 2022:
  - Installation of new CVES mobile units completed
  - Hosted local PD mobile tenants completed
- June 2022:
  - Second round of Boss4 software upgrades completed by vendor (Q2)

U//LES - Do Not Disseminate

ALPR Hardware

- Department's current LPR camera vendor is Neology
- Cameras have been operating for years; many are end-of-life
    - Numerous units (Cape especially) are at risk of failure due to age
- Deployed camera technology is outdated
- Models with improved performance and accuracy are available
- Department's Wanco solar trailers are aging and in need of upgraded solar panels and batteries in order to work overnight

U//LES - Do Not Disseminate

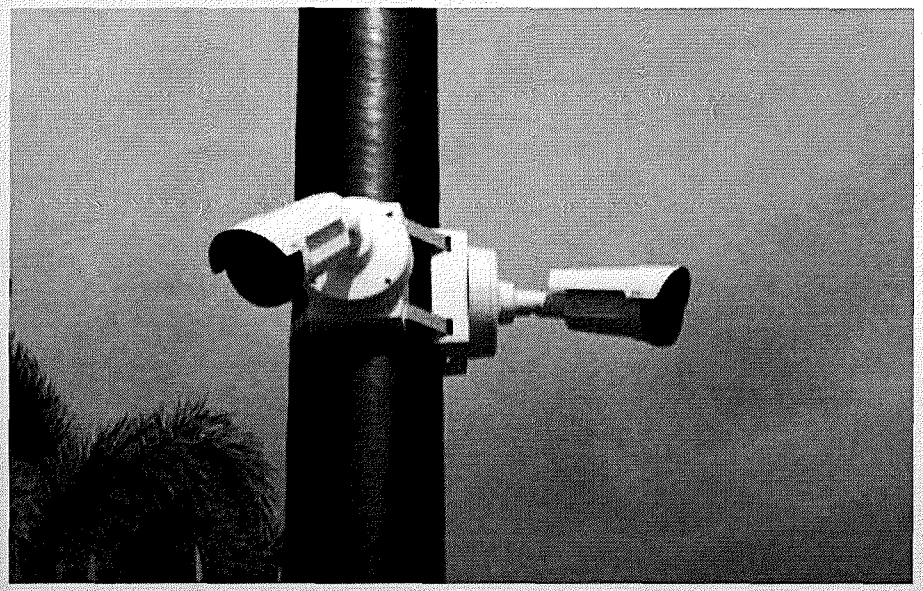
State of the Industry

U//LES - Do Not Disseminate

State of the Industry

- LPR technology has grown rapidly over the past few years
- New venders have made it technically accessible and financially affordable for local departments to deploy LPRs in their communities

Rekor





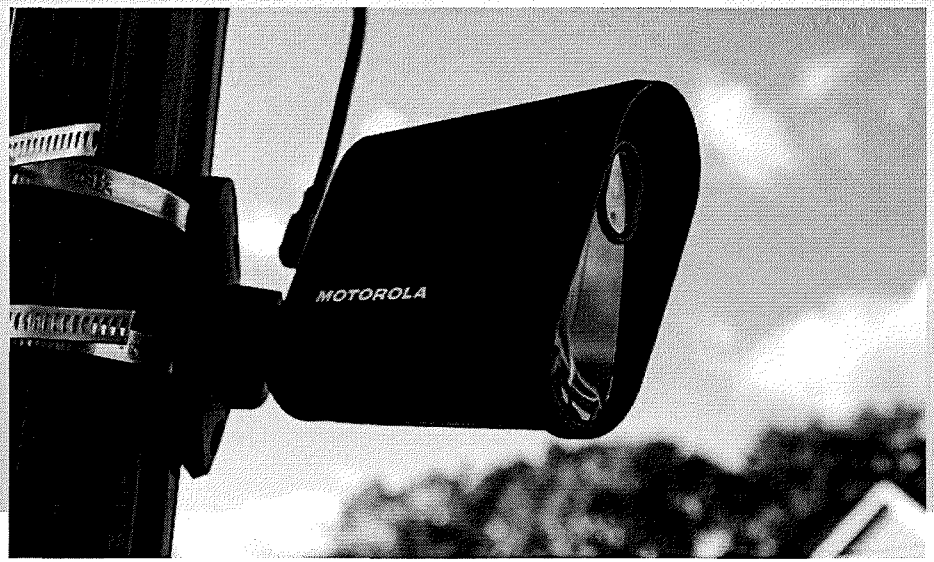
Flock

U//LES - Do Not Disseminate

In our Region

- Motorola/Vigilant in about 6 communities in MA
- Flock in about 15-20 communities in MA
- Rekor growing in CT
- CSP: expected to on board with Rekor in near future
- NYSP: recent switch to Vigilant, [redacted] permanent locations, adding [redacted] this year
- Numerous communities running various mobile LPR systems

Motorola/
Vigilant



U//LES - Do Not Disseminate

Future of MSP's Program

U//LES - Do Not Disseminate

Program Goals
2022 and beyond

- Support the Department's Homeland Security mission and improve real-time response capabilities to emergency situations, including:
  - AMBER and SILVER alerts
  - Locating missing, endangered, or kidnapped persons
  - Preventing and investigating terrorism threats and incidents
  - Major crime response and investigation
- Ensure that the Commonwealth Watch Center has the training and tools necessary to use ALPR technology in support of this mission
- Identify critical infrastructure, high-risk public events, and major highway locations where ALPR equipment can be deployed in support of this mission

U//LES - Do Not Disseminate

Program Goals
2022 and beyond

- Develop partnership with MassDOT for collocating equipment
- Increase regional cooperation, communication, and data sharing with partner agencies regarding LPR use and best practices
- Ensure that MSP has sound, modern, and lawful policy and practices
- Serve as a model for other states and local partners in both policy and professional utilization of technology in the modern era
- Update and replace aging equipment to maintain current level of services

U//LES - Do Not Disseminate

Equipment Upgrades
Available Funding

- Funding is available to replace and upgrade LPR equipment
  - *Federal High Priority grant to CVES:* approximately $800,000 for mobile units; $700,000 spent for 26 new mobile units, about $100,000 remaining
  - *Fusion Center grant:* approximately $500,000 to replace trailers and cameras
  - *Methamphetamine/heroin grants:* approximately $200,000 for LPR equipment
  - *Traffic Programs grants:* approximately $50,000 to repair mobile units
  - *HIDTA:* $40,000 previously spent end of 2021 to order 5 replacement cameras
- Benefits of replacement equipment:
  - Replacement trailers: better solar and batteries, hopefully 24-hour operation
  - Replacement cameras: better analytics with improved read accuracy
  - Repair of mobile units: potentially redeploy some old equipment to support DFS

U//LES - Do Not Disseminate

Equipment Deployments

- Solar trailers (hopefully replacements) will be redeployed in spring
- Major public events, i.e., Boston Marathon and Esplanade
- Under consideration for improved or future deployments include:
  - Critical infrastructure: G.L. c. 4.sec. 7.cl.26 (n)(security)
  - Major highways, especially at G.L. c. 4.sec. 7.cl.26 (n)(security) have previously used trailers and would benefit from a more reliable system)
- Our LPR system cannot be significantly expanded without additional cellular data plans
  - Each site needs at least one cellular data plan
  - Data plans cannot be purchased using grant funding

U//LES - Do Not Disseminate

Effective Date:	Number:
November 10, 2021	**TRF-11**
Subject: **Automatic License Plate Recognition**	

Policy
Review & Modernization

- Department has a thorough ALPR policy
- Policy updates may be considered to provide additional protections that are mindful of trends in technology use by police
- Federal and state courts generally do not consider LPR use to be a search, including SJC in Commonwealth v. McCarthy (2020)
- However: McCarthy decision hints that our courts may want to be the first

U//LES - Do Not Disseminate

Goals of Review

1. Reduce privacy risk: retention and access
2. Identify areas where policy can be modernized
3. Retain and improve system utility for exigent situations and major investigations

U//LES - Do Not Disseminate

Discussion
Risk Mitigation

- Privacy
- Retention
- Access
- Modernization

U//LES - Do Not Disseminate

Discussion
Privacy

Privacy considerations were reviewed to identify policy and practice adjustments that may improve privacy protections:

- Manual entries to a hotlist could be authorized by a supervisor, removed as soon as possible, and limited to 30 days (reduced from 1 year; some exceptions)
- Historical searches could be limited to the geographic search area as reasonable to investigation and the time window limited to 30 days (reduced from 1 year; some exceptions)
- Training for users could be required to include discussion of privacy considerations and minimization

U//LES - Do Not Disseminate

Discussion
Access

Access to the system is a factor that may affect the privacy risk of an LPR program

- Restricting access too far lowers usefulness as a public safety tool
- Access adjustments to improve privacy protections may include:
  - Watch Center could be designated as a primary LPR resource, which would enable consistent use practices, documentation, and data entry
  - Access could be designated at the unit supervisor level, either on a shall-issue or specific-need basis
  - Access of Troopers and dispatchers could be reduced to a core group with advanced training, or additional restrictions placed on their system use

U//LES - Do Not Disseminate

Discussion
Data Retention

Length of time that LPR data is retained is a primary privacy consideration

- MSP data is currently held for one year based upon DCJIS/EOPSS policy
- *"The one-year retention period...certainly is long enough to warrant constitutional protection."* Commonwealth v. McCarthy
- LPR system is soon to be under Department control, and it may be time to re-evaluate the retention period
- Issues with one-year retention period:
  - Privacy vs. utility balance may be skewed
  - Higher data storage costs and fewer viable vendors

U//LES - Do Not Disseminate

Discussion

Data Retention (Continued)

- Data retention settings are managed at the administrative level in new software
- Data retention time for discussion: **90 days**

Benefits of 90-day data retention vs. 1-year retention:

- 75% reduction in storage time is an articulable privacy improvement
- Majority of investigative value is retained
- Reduces operating costs and allows consideration of new vendors
- Brings retention closer in line with other agencies

- A time period shorter than 90 days might reduce system usefulness too far, and a policy provision that restricts searches and manual hotlist entries to 30 or 45 days could still be added to serve as additional protection

U//LES - Do Not Disseminate

Discussion
Modernization

Additional areas to consider for update and modernization could include:

- An explicit notice to export records for preservation and discovery
- Accounts with outside LPR systems must be authorized and follow policy
- Authorized LPR system uses:
  - Authorized uses could exclude certain low-level offenses
  - System use for immigration enforcement could be explicitly prohibited
  - Allowance to use for MV pursuit follow-up investigations could be added

U//LES - Do Not Disseminate

Summary

- Seeking to modernize the Department's ALPR program, from equipment to policy
- Grant funding is available to replace/upgrade equipment
- Transition to new system is bumpy but progressing
- Technology use is expanding, and interagency cooperation will be increasingly important to keep the Department as the premier investigative resource agency in the state
- Policy recommendations will be forwarded in coming months

U//LES - Do Not Disseminate

References

- American Association of Motor Vehicle Administrators. (2021). *License Plate Reader Program Best Practices Guide.*
- Commonwealth vs. Jason J. McCarthy, 484 Mass. 493 (2020).
- Department of State Police. (2021). General Order TRF-11.
- Rand Corporation Safety and Justice Program. (2019). *License Plate Readers for Law Enforcement: Opportunities and Obstacles.*

U//LES - Do Not Disseminate